UNIVERSITÉ DE MONTRÉAL

L'ORIGINE GÉOGRAPHIQUE EN TANT QUE FACTEUR EXPLICATIF DE LA CYBERDÉLINQUANCE

PAR
MIRA CARIGNAN

ÉCOLE DE CRIMINOLOGIE
FACULTÉ DES ARTS ET DES SCIENCES

MÉMOIRE PRÉSENTÉ À LA FACULTÉ DES ÉTUDES SUPÉRIEURES
EN VUE DE L'OBTENTION DE M.SC.
EN CRIMINOLOGIE

SEPTEMBRE, 2015

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé :
L'origine géographique en tant que facteur explicatif de la cyberdélinquance

Présenté par
Mira Carignan

A été évalué par un jury composé des personnes suivantes :

Benoit Dupont
directeur de recherche

Francis Fortin
Membre du Jury

Chloé Leclerc
Membre du jury

RÉSUMÉ

Ce mémoire propose que l'origine d'un cyberdélinquant soit un facteur explicatif du phénomène de la cybercriminalité. Il comporte deux objectifs : premièrement, décrire les profils des cybercriminels recensés dans les médias internationaux; deuxièmement, vérifier si ces profils varient selon le lieu d'origine du cyberdélinquant. Une base de données, comportant 90 cas de cybercriminels répertoriés à travers le monde, fut créée. Quinze (15) cybercriminels par territoire ont été sélectionnés, les régions ciblées allant comme suit : Amérique du Nord, Amérique latine, Australasie, Europe de l'Ouest, Eurasie et Afrique/péninsule Arabique. En premier lieu, des analyses descriptives ont été exécutées afin de dresser un portrait de ce phénomène. En second lieu, des analyses de tableaux de contingence ont été effectuées entre les variables à l'étude afin de voir si des relations existaient. Enfin, d'autres analyses de tableaux de contingence ont été réalisées afin d'établir les différences des paramètres en fonction de l'origine. Les résultats de ces divers tests démontrent que ce sont généralement de jeunes hommes âgés en moyenne de 25 ans qui seront susceptibles de commettre des délits informatiques. Quelques profils types se sont dégagés des analyses et peuvent s'expliquer par l'accès au matériel informatique, les inégalités économiques entre classes sociales, tout comme la vitesse d'Internet, et ce, en fonction de l'origine du cyberdélinquant.

Mots-clés : hacker, pirate informatique, cybercrime, cybercriminalité, cybercriminel, cyberdélinquant, origine, territoire, région

ABSTRACT

This memory suggests that the origin of a cybercriminal is an explanatory factor of the phenomenon of cybercrime. It has two specific objectives: first, to describe the profile of cybercriminals identified in the international media. It also aims to check whether these profiles vary according to the origin of the cybercriminal. A database was created, with 90 cases of cybercriminals, worldwide. Fifteen (15) cybercriminals were selected per geographical territories, areas ranging as follows: North America, Latin America, Australasia, Western Europe, Eurasia, and Africa/Arabian Peninsula. First of all, descriptive analyzes were performed in order to paint a picture of this phenomenon. Secondly, analyzes of contingency tables were performed between the variables being studied to see if relationships existed. Finally, other analyzes of contingency tables were performed to establish the differences of the parameters depending on the origin. The results of these tests reveal that it is in general young men with an average age of 25 who will commit computer crimes. Some typical profiles emerged from the analysis and can be explained by access to computers, Internet speed, and inequalities in economic distribution, depending on the origin of the cybercriminal.

Mots-clés : hacker, cybercriminal, cybercriminality, cybercrime, cyberdelinquency, origin, territories, region

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES SIGLES ET ABRÉVIATIONS

Afr/pénin.....Afrique/péninsule Arabique

Amlatine ..... Amérique latine

AmNoRD .....Amérique du Nord

Austral.....Australasie

Comm.États indépendants..... Communauté des États Indépendants

DOS ..... Denial of service

EurOuest ..... Europe de l'Ouest

OECD .....The Organisation for Economic Co-operation and Development

OQLF ..... Office québécois de la langue française

UNODC..... United Nations Office on Drugs and Crime

REMERCIEMENTS

Les remerciements sont pour moi difficiles, par peur d'oublier ou de froisser quelqu'un. Je suis normalement une personne positive qui va de l'avant. Durant la rédaction de ce mémoire, des obstacles ont freiné mon optimisme; j'ai parfois pensé à tout arrêter, mais j'ai un entourage extraordinaire qui a su m'écouter et me soutenir.

D'abord, merci à mon directeur de recherche, Benoit, qui, malgré son engagement dans de nombreux projets, a su me consacrer du temps, tout comme me redonner confiance dans les moments où elle manquait. Merci d'avoir accepté de prendre en charge un tel projet.

Ces remerciements seraient vides, si je ne remerciais pas ma famille. Merci à mes sœurs Virginie, Justine et Laurie, ainsi qu'à ma mère, Monique, qui m'ont encouragée et qui m'ont donné la tape dans le dos, lorsque nécessaire. Merci à ma mère et à mon père, qui m'ont permis de me rendre jusqu'aux études supérieures.

Merci également à mon copain Carl qui m'a soutenue ces deux dernières années, qui m'a comprise et qui a assumé beaucoup de tâches lorsque j'étais hypnotisée par mon écran d'ordinateur et qui m'a endurée dans des moments moins «jojo», où la patience n'était pas à son plus haut niveau. Merci de m'avoir aidée et encouragée. Merci de ta présence chaque jour, de ta patience et de toutes tes petites attentions qui m'ont supportée et qui ont rendu mon quotidien plus agréable.

Merci à mes amis (es) que j'ai délaissés trop longtemps, mais qui ont saisi l'importance de ce mémoire et qui ont su m'apporter du courage. Merci d'être restés là, à mes côtés, malgré ma presque négligence. Merci Esther, Vanessa, Naomi, Jeremy, Geneviève, Mylène, Valérie et Ariane. Merci d'avoir compris.

Merci à une amie spéciale, avec qui j'ai passé de nombreuses heures dans les cours, à étudier, à rédiger le mémoire, avec qui j'ai pu vider mon fiel et laquelle m'a toujours apporté un sourire lorsque j'en avais besoin, de par son humour et sa joie de vivre. Merci ma belle Audrey. Sans toi et sans ces moments de rigolade et de laisser-aller, la maîtrise n'aurait pas été aussi agréable!

Sans oublier les remerciements à mes collègues de travail, merci pour votre compréhension tout au long de la dernière année et pour m'avoir écoutée tout ce temps. Merci.

Finalement, merci à tous ceux, de près ou de loin, qui m'ont appuyé et qui m'ont donné le courage de mener à bien ce mémoire

INTRODUCTION

L'utilisation des ordinateurs, des portables ainsi que des téléphones intelligents fait maintenant partie intégrante des sociétés au plan international en plus de faire des adeptes de plus en plus jeunes. Effectivement, une proportion croissante de la population est plus encline à faire usage d'Internet, principalement entre 16 ans et 24 ans, et ce, contrairement à la population âgée de plus de 65 ans, pour laquelle l'utilisation d'Internet se fait plutôt rare (l'OECD Internet Economy Outlook, 2012). De plus, le besoin que ressent la population à recourir à Internet est grandissant. Selon le rapport de Norton (2011), 24% des adultes au niveau mondial affirment qu'ils «ne peuvent vivre sans Internet» et 41% de la population adulte faisant usage d'Internet assure que c'est un besoin dans la vie de tous les jours.

Comme beaucoup d'individus utilisent leurs appareils technologiques afin d'acheminer leurs courriels, leurs transactions bancaires, leurs achats en ligne ainsi qu'à des fins de loisirs, une forme de criminalité s'est amplifiée au même rythme que les propensions pour le numérique ainsi que le déploiement même de la technologie, et ce, majoritairement grâce à Internet. Le nombre de crimes informatiques serait proportionnel à l'usage qu'en fait la population (Holt et Kilger, 2008). En effet, «la vitesse d'Internet en est devenue sa faiblesse» (McCusker, 2007). La facilité d'accès à Internet offre de meilleures opportunités criminelles dans le cyberespace (Britz, 2008), dans un monde virtuel où il n'existe encore aucune autorité en mesure de les contraindre et où les autorités classiques, comme la police, sont plutôt démunies (UNODC, 2013). L'étude de l'OECD Internet Economy Outlook (2012) vient d'ailleurs soutenir ces propos. Ils se sont basés sur les différents mécanismes de classification que les chercheurs de cette étude ont établis, notamment les impacts directs, dynamiques et indirects d'Internet sur l'économie générale. Effectivement, elle soulève par exemple que l'intégrité des informations confidentielles des

différentes entreprises est de plus en plus menacée par l'augmentation de l'utilisation des logiciels malicieux, des DOS (denial of service) ou autre. D'ailleurs, 94,4% des entreprises de l'Union européenne étaient connectées à Internet en 2010 (OECD Internet Economy Outlook, 2012).

Malgré l'accroissement de ce type de criminalité, il existe peu d'analyse sur la cybercriminalité et la piraterie informatique, outre les études en lien avec le profil type du pirate (Meyer, 1989; Hollinger, 1990; Rogers, 2006; Young, Zhang et Prybutok, 2007; Chiesa, Ciappi et Ducci, 2007; Leeson et Coyne, 2005) et les caractéristiques du crime (Meyer, 1989; Hollinger; 1991; Jordan et Taylor, 1998; Nissenbaum; 2004). Il en existe encore moins ayant pris en compte la provenance du délinquant ou le pays d'origine de celui-ci en tant que facteur explicatif. Pourquoi en est-il ainsi? Il est depuis longtemps assumé par la société que les crimes informatiques ne varieraient pas tellement en fonction du pays d'origine puisque la technologie avance généralement au même rythme d'un pays à l'autre. Donc, les caractéristiques définissant les pirates informatiques seraient considérées les mêmes à l'échelle mondiale. Effectivement, les types de crimes et de délits en matière informatique sont peu variés, de par l'universalisme d'Internet. Par exemple, les plateformes informatiques seront accessibles à tous les cybercriminels ayant un accès à Internet, et ce, à travers le monde. Ceci fait en sorte que la cybercriminalité est encore plus homogénéisée par la société et qu'aucune attention particulière n'est portée à l'approfondissement des questionnements.

Or, ce mémoire, à but exploratoire, vise à contrer ce manque au niveau des recherches scientifiques quant à la cybercriminalité. Il propose que l'origine d'un cyberdélinquant soit un facteur explicatif du phénomène de la cybercriminalité. Deux objectifs y sont ciblés : soit d'abord de décrire le profil des cybercriminels recensés dans les médias internationaux, soit il

vise de vérifier si ces profils varient selon le lieu d'origine du cyberdélinquant. Effectivement, en quoi est-ce qu'une société ou l'origine d'un délinquant peuvent-elles influencer les caractéristiques du crime, les caractéristiques personnelles des cyberdélinquants ainsi que les particularités motivationnelles? La rapidité d'Internet ainsi que l'accès aux outils technologiques seront-ils des éléments en lien avec ce phénomène ainsi que les traits distinctifs criminels? Ce mémoire vise à répondre à ces questions. Il est tout de même possible de supposer que les opportunités criminelles créées par l'environnement auront effectivement un impact sur les choix des cyberdélinquants.

Les cadres théoriques existant sur le sujet de la cybercriminalité ne semblent pas s'intéresser à la provenance géographique des pirates informatiques et aux implications de celle-ci sur leurs motivations et leurs activités. Comme la recherche se veut exploratoire, ce mémoire s'inspire néanmoins de cadres théoriques, de travaux et de typologies déjà existantes sur le profil des pirates. Le mélange de ces typologies est créé dans le but d'assumer une certaine continuité, tout en englobant les critères importants et spécifiques à ce type de criminalité. Par exemple, la typologie de Holt et Bossler (2014) est utilisée pour le type de crime, les catégorisations de Jordan et Taylor (1998), Rogers (2006) ainsi que Chiesa, Ciappi et Ducci (2007) sont combinées pour le type de motivation et la typologie du degré de compétence réalisée dans l'étude de Verizon (2012) servira de guide dans nos analyses. Les autres catégorisations furent créées dans le cadre de la présente étude. Également, la dimension géographique reste pertinente, même pour des formes de délinquance dématérialisées et ce, dans une optique de prévention situationnelle. Effectivement, ce mémoire aura pour effet de cibler divers types de cyberdélinquances, de motivations ou même les

types de victimes et ce, en lien avec l'origine du délinquant, ce qui pourra aider de futurs chercheurs à créer des outils pour pallier ce type de criminalité.

Le corps de cet ouvrage est composé de cinq (5) chapitres. D'abord, le lecteur trouvera une recension des écrits en lien avec le phénomène de la cybercriminalité. Ce premier chapitre consiste d'abord à identifier les profils des cybercrimes. Plus précisément, il aborde les définitions et caractéristiques des types de crimes et les conséquences de la cybercriminalité. Il aborde également le profil des communautés et les caractéristiques sociales des cyberdélinquants. Ensuite, ce chapitre vise à identifier le profil des cybercriminels, notamment les caractéristiques démographiques, les motivations de celui-ci, le degré de compétence du délinquant et l'aspect psychologique de ce dernier. Le lecteur trouvera aussi dans ce chapitre la littérature s'étant intéressée au phénomène, notamment les limites de ces dernières. Seront ensuite présentés la problématique, les objectifs de l'étude et les profils des cyberdélinquants identifiés. Le second chapitre expose la méthodologie de notre étude, soit l'explication de la formation de notre source de données tout comme les limites rencontrées lors de la création de cette base de données, l'opérationnalisation des variables à l'étude ainsi que la stratégie analytique adoptée. Le troisième chapitre révèlera les résultats des tests statistiques descriptifs et le quatrième chapitre ceux des tests statistiques bivariés de tableaux de contingence. Finalement, le cinquième chapitre vise à interpréter ces résultats, chapitre qui sera suivi d'une conclusion.

CHAPITRE 1 : RECENSION DES ÉCRITS

Ce chapitre, basé sur une recension des écrits portant sur la cybercriminalité brosse un portrait de ce type de criminalité trop peu analysé par les chercheurs. Il sera divisé en quatre sections, soit le profil des cybercrimes, le profil des communautés, le profil des cybercriminels, la littérature s'étant intéressée au phénomène et finalement, la problématique à l'étude.

1.1 PROFIL DES CYBERCRIMES

Avant d'émettre des pistes de recherche ou même d'établir la problématique, il est important de bien décrire ce phénomène, d'avoir une idée de l'ampleur ce celui-ci au niveau mondial en créant un portrait statistique, ainsi qu'en faisant la recension des études s'étant intéressées à cette criminalité au point de vue international. Cette première section permettra au lecteur de comprendre pourquoi il est pertinent d'approfondir les connaissances sur ce sujet. D'abord, voici les définitions des termes quant à ce phénomène qu'est le cybercrime.

1.1.1. Définitions et caractéristiques des types de crimes

Avant de se lancer dans l'énumération de divers types de crimes, voici la définition du grand dictionnaire terminologique de l'Office québécois de la langue française (OQLF, 2015) de ce qu'est la cybercriminalité : «Criminalité informatique associée au cyberespace, qui recouvre l'ensemble des infractions pénales commises au moyen du réseau Internet». Quant au cybercrime, il est défini comme un «acte illicite commis au moyen de l'informatique, ou ayant pour cible le système informatique ou l'un de ses éléments» (OQLF, 2015).

Ensuite, une clarification de certains termes informatiques est de mise. Un lien est créé par divers auteurs entre ces deux notions : la piraterie informatique et le «hacking». Bien qu'il soit commun de les intégrer dans la même catégorie, ces deux actes ne sont en fait pas définis de la même manière (Schell et Martin, 1952; Meyer, 1989; Wall, 2003). En effet, pirater est le fait de «copier et distribuer, sans autorisation préalable, des logiciels avec des droits d'auteurs» (Meyer, 1989 p.28; Turgeman-Goldschmidt, p. 385, 2008). Selon le grand dictionnaire terminologique de l'Office québécois de la langue française (2015), il est défini comme un «délit informatique qui consiste à s'approprier un concept logiciel en vue d'une exploitation ultérieure, à violer l'intégrité d'un système dans un but malveillant ou à copier des informations sans permission pour les diffuser ou les vendre». Ainsi, il ne s'agit pas d'infiltration dans les systèmes, mais bien d'un partage illégal suite à une copie d'informations protégées par le droit d'auteur. Pour ce qui est du «hacking», il est défini comme étant «l'accès non autorisé ou l'utilisation subséquente du système de l'ordinateur d'autres personnes» (Meyer, 1989, p.20; Turgeman-Goldschmidt, 2008, p.386). Selon le CSI Computer Crime and Security Survey de 2010-2011 (Richardson, 2011), plus de 30% des incidents informatiques consistent en des accès non autorisés à des systèmes informatiques (N=351). Les questionnaires de cette étude ont été distribués à des individus pratiquant dans le domaine de la sécurité informatique tout en demeurant anonymes. La piraterie informatique ainsi que le «hacking» sont donc des termes intéressants à dissocier. Dans le cadre de notre étude, il sera question de cybercrime, cyberdélinquance, cyberdélinquants ou de délinquants informatiques, incluant la piraterie informatique et le «hacking», afin d'éviter toute confusion. En d'autres termes, la piraterie informatique inclura le piratage informatique ainsi que le «hacking», et ce, dans le but de faciliter la lecture de ce mémoire tout en évitant de confondre les termes.

Il est pertinent de soulever les éléments communs des diverses typologies quant aux caractéristiques du crime informatique puisqu'elles serviront de guide au cours de l'étude actuelle (Wall, 2003; Jordan, 2008; Holt et Bossler, 2013). En premier lieu, il y a l'infiltration. C'est, selon le grand dictionnaire terminologique de l'OQLF, une «opération qui consiste à accéder, sans autorisation, à un système informatique ou à un réseau, en contournant ou en désamorçant les dispositifs de sécurité mis en place». Ce premier type de crime suppose les virus informatiques ainsi que leur création, les attaques informatiques, les robots informatiques, les logiciels malveillants, ainsi que les infiltrations informatiques. Les robots informatiques sont, selon Microsoft (2014), «des logiciels malveillants capables de transformer un ordinateur en « bot » (également appelé zombie). Le cas échéant, l'ordinateur peut réaliser des tâches automatisées sur Internet sans que la victime ne le sache». Selon le CSI Computer Crime and Security Survey de 2010-2011 (Richardson, 2011), 29% des expériences de délits informatiques étaient des « bots », 67% des infections par logiciels malveillants.

En deuxième lieu est cité le cybervol. Celui-ci implique la fraude ainsi que les vols de données personnelles, pour ainsi dire tous les délits entraînant des profits. Selon le CSI Computer Crime and Security Survey de 2010-2011, 9% des délits informatiques étaient qualifiés de frauduleux en 2010 (Richardson, 2011). Le cybervol inclut aussi le «phishing», soit l'hameçonnage. Cette forme de criminalité peut être utilisée par des individus ayant un faible degré d'habiletés informatiques (Herley et Florêncio, 2008). C'est par définition «un courriel imitant le logo de l'entreprise offrant un service, visant à attirer les utilisateurs non avertis sur de faux sites imitant l'original, où ils entrent leurs données personnelles qui seront conservées dans un serveur» (Birk,

Gajek, Grobert et Sadeghi, 2007, p.2). Ainsi, il y aura fraude des consommateurs ciblés par le cybercriminel, fournissant d'eux-mêmes leurs informations confidentielles (Jagatic, Johnson, Jabobsson et Mencser, 2007). Selon le CSI Computer Crime and Security Survey de 2010-2011 (Richardson, 2011), 39% des entreprises formant l'échantillon étaient faussement représentées dans des courriels d'hameçonnage. Troisièmement, il y a la cyberpornographie ou obscénité. Elle est définie par l'OQLF (2015) comme la «pornographie diffusée par les réseaux d'Internet et qui consiste surtout à présenter des collections d'images, d'animations ou de vidéos obscènes réduisant la sexualité à de grossières représentations limitées exclusivement à la génitalité». Celle-ci tient compte de la pornographie, la sollicitation à la pornographie ou à des actes sexuels, bref, tous les délits reliés à une quelconque déviance sexuelle (Wall, 2003). Le dernier type de crime énuméré dans cette typologie est la cyberviolence. Elle implique le cyberterrorisme, défini selon le grand dictionnaire terminologique de l'OQLF (2015) comme l'«utilisation de l'information et du contrôle des systèmes d'information, par des groupes organisés ou par un individu, comme arme stratégique pour exercer des pressions et intimider l'adversaire». Elle inclut aussi la cyberintimidation, soit les «actes répétés d'agression psychologique commis par un individu, ou par un groupe d'individus, qui rejoint ses victimes par l'intermédiaire du réseau Internet, du courriel, de la messagerie instantanée ou textuelle» (OQLF, 2015), ainsi que le harcèlement.

Bref, cette typologie permet de mieux distinguer les cybercrimes, qui ne couvrent cependant pas toutes ces catégories puisque ces dernières sont principalement limitées aux infiltrations. De ce fait, dans le cadre de l'étude actuelle, les attaques informatiques seront évaluées de façon distincte des infiltrations, parce qu'elles sont de plus en plus importantes et prisées par les cybercriminels. Également, ces deux délits qui ont des répercussions différentes, requièrent des niveaux de

compétences différents et sont parfois perpétrés selon des motifs différents. D'ailleurs, les attaques informatiques consistent en des virus, botnets et logiciels malveillants qui peuvent facilement être lancés dans un système informatique par des individus ayant un faible degré de compétence ou tout simplement aucun degré de compétence. Ils peuvent les trouver via Internet et ainsi les répandre pour causer plusieurs dommages destructifs, notamment en matière de réparation. Leur motif peut, par exemple, être de nature de revanche (Rogers, 2006). Toutefois, certains pirates informatiques plus avancés pourront créer ces logiciels ou virus par eux-mêmes. En ce qui a trait à l'infiltration, elle demande un degré de compétence informatique plus élevé, notamment en ce qui concerne les connaissances techniques nécessaires. De plus, le motif idéologique (Nissenbaum, 2004; Chiesa, Ciappi et Ducci, 2007) ou financier (Copes et Viaraitis, 2004) du cyberdélinquant prévaudrait dans le cas des infiltrations informatiques, dans le but de faire passer un message, de retrouver des données confidentielles, etc.

Bien que les typologies soient semblables en ce qui a trait au type de délit, de nombreux chercheurs emploient des méthodes différentes pour mener à bien leurs études. Effectivement, certains distribuent des questionnaires dans de grands forums de « hackers » afin d'aller chercher les renseignements directement, notamment quant à leurs modes opératoires, leur motivation et leurs objectifs. Certains se fieront aux données plus officielles des entreprises de logiciels de protection afin d'étudier quels sont les cyberdélits les plus fréquents, par exemple, les délits de fraudes, d'hameçonnage, d'infiltration, etc. D'autres vont étudier les conséquences en faisant des sondages téléphoniques auprès d'individus dans la population afin de les questionner sur leurs méthodes de protection ou pour savoir s'ils ont déjà été victimes d'un délit, et si oui, lequel. Les crimes sont donc

analysés différemment d'une étude à l'autre. Afin de bien situer le lecteur, des explications sur les processus d'analyses seront incorporées au fil de la lecture.

Il est intéressant de connaître les divers types de délits connus quant à la cybercriminalité, mais l'importance et la gravité de ces derniers sont encore peu connues. Conséquemment, voici quelques chiffrages à cet effet.

1.1.2.Conséquences de la cybercriminalité

De prime abord, il est pertinent de donner une idée générale de l'ampleur du phénomène de la cybercriminalité en relevant les statistiques qui en chiffrent le coût. D'abord, l'étude effectuée par Norton (2011) établit les coûts de la cybercriminalité à 388 milliards de dollars US$. En ce qui a trait aux coûts reliés à la perte de temps des victimes, en termes de démarches et de prévention, ils s'élèvent à 274 milliards US$. Finalement, les coûts directs, soit plus particulièrement l'argent ayant été subtilisé ainsi que l'argent mis au profit de la réparation des torts causés, sont estimés à 114 milliards US$ mondialement. Afin d'obtenir ces résultats, l'équipe de Norton a distribué un questionnaire dans 24 pays différents, interrogeant des enfants (N=4 553), des parents (N=12 704) et des enseignants d'élèves âgés de 8 à 17 ans (N=2 379), générant un total d'entretiens de N=19 636. Les mêmes questions étaient posées d'un pays à l'autre, dans la langue maternelle afin d'en faciliter la compréhension. À prendre en compte que «les données globales ont été pondérées pour s'assurer que tous les pays aient une représentation globale» (Norton, 2011). Dans cette étude, la cybercriminalité est nommée comme étant

> «au moins un des préjudices suivants : Des virus informatiques ou logiciels malveillants sont apparus sur mon ordinateur, j'ai répondu à un message d'hameçonnage en pensant que

> c'était une demande légitime, harcèlement en ligne, quelqu'un a piraté mon profil de réseau social et s'est fait passer pour moi, j'ai été approché en ligne par des prédateurs sexuels, j'ai répondu à des escroqueries en ligne, j'ai été touché par une fraude à la carte de crédit, on a usurpé mon identité, j'ai répondu à un message de smishing (hameçonnage par messagerie texte téléphonique), j'ai été atteint par un autre type de cybercriminalité sur mon téléphone mobile, j'ai été atteint par un autre type de cybercriminalité sur mon ordinateur» (diapositive 9; méthodologie et définitions).

De plus, les coûts reliés à l'hameçonnage s'élevaient en 2007 à 473,28 millions US$, tandis qu'ils étaient de 6 211,80 millions US$ en 2010 pour des fraudes de cartes de crédit en ligne et de 1 479 millions $US pour des fraudes d'avances financières en 2011. Ils étaient moindres en ce qui a trait aux logiciels malicieux chez les consommateurs, somme évaluée à 103,53 millions $US en 2010 (Anderson et coll., 2013). Les coûts défrayés pour le nettoyage de l'ordinateur chez les utilisateurs et pour la défense des entreprises en général s'élevaient à 14 790 millions $US chacun. À noter que les coûts engendrés uniquement par l'obtention d'un antivirus s'élevaient en 2012 à 5 028,60 millions $US. Bref, la cybercriminalité ne semble pas être un délit à prendre à la légère compte tenu des lourdes conséquences financières qu'elle entraîne.

Ainsi, il est possible d'observer, bien qu'il y ait une sélection restreinte de la criminalité dans cette étude, que les coûts globaux engendrés par la cybercriminalité sont considérables et que celle-ci a conséquemment un impact réel dans la société, pour lequel une attention particulière doit être portée. Ensuite, afin de bien se situer au niveau de la croissance de ce phénomène technologique, voici le contexte d'adoption des nouvelles technologies. L'Union Internationale des télécommunications (2014) a fait une recension du nombre d'individus adoptant des outils technologiques et de communication au fil des années, et ce, par régions. Les données de leur étude ont été recensées suite à la distribution de questionnaires envoyés sur une base annuelle auprès d'environ 200 pays et régions économiques. Ce sont des institutions spécialisées qui produisent des

statistiques couvrant leur domaine d'opération respectif et qui font partie du système statistique mondial de l'ONU et qui se chargent de colliger les données. La recension dévoile des chiffres en fonction des pays développés et ceux en voie de développement.

D'abord, il est possible d'observer que les ménages originaires des pays développés sont beaucoup plus nombreux à posséder des ordinateurs à la maison que les pays en voie de développement. D'ailleurs, non seulement ce constat se reflète quant à la possession de l'ordinateur, mais aussi quant à l'accès à Internet à la maison. Enfin, les résultats de cette étude illustrent bien l'augmentation de la propension de l'usage d'Internet au fil des années, et ce, en considération des différentes régions. Effectivement, en 2005, 44,7 par 100 habitants avaient accès à Internet à la maison dans les pays développés, comparés à 78,4 en 2014. Quant aux pays en développement, 8,1% des ménages avaient accès à Internet à la maison en 2005, comparé à 31,2% en 2014 (L'Union Internationale des télécommunications, 2014).

Ces différentes statistiques nous permettent d'observer cette propension de plus en plus évidente de l'utilisation d'objets technologiques tout comme l'usage d'Internet, et ce, à travers le monde. Il est aussi intéressant d'observer certains schèmes régionaux et différences régionales. Au niveau de la possession d'un ordinateur, il semble que les pays d'Afrique soient les moins enclins à en posséder (L'Union Internationale des télécommunications, 2014). L'accès aux technologies, restreint en Afrique, aurait probablement un effet sur l'accès à Internet. D'ailleurs, c'est une des régions ayant l'accès le plus réduit à Internet, tout comme les États arabes et la communauté des États indépendants (incluant les anciennes républiques de l'Union Soviétique), et ce, loin derrière les autres territoires. Ces différentes régions sont marquées par certains territoires présentant une

économie plus précaire, pouvant expliquer ce faible accès aux technologies et à Internet. Toujours selon l'Union Internationale des télécommunications (2014), les individus en provenance de l'Europe et des Amériques sont ceux ayant le meilleur accès à Internet. La cybercriminalité des délinquants en provenance de ces territoires géographiques sera-t-elle plus complexe et élaborée que celle des délinquants d'Afrique, de par l'accès aux outils technologiques et l'accès à Internet? L'étude actuelle tentera d'en découvrir davantage.

Plusieurs questionnements sont aussi soulevés quant aux auteurs des délits informatiques. D'emblée, il serait approprié de distinguer les menaces de sources externes et les menaces de sources internes, où ces deux approches entraînent des moyens de prévention totalement différents. Les menaces d'origines externes proviennent «des utilisateurs situés en dehors du système d'information» d'une compagnie, d'une entreprise ou même d'un gouvernement (gouvernement du Canada, 2014). Une menace interne est «une menace malveillante et souvent criminelle contre un organisme public ou privé qui émane d'une personne œuvrant à l'intérieur de l'organisme» (gouvernement du Canada, 2014). Dans 68% des cas de cybercriminalité ayant pour cible les sociétés commerciales ou les entreprises, le malfaiteur était un employé de celles-ci (Hollinger, 1991; Telus-Rotman, 2013). Ce même constat se reflète dans l'enquête de l'Association des membres du Barreau américain (1984) menée auprès de 283 entreprises et organisations, notamment des entreprises bancaires et financières, des entreprises informatiques et des départements et agences majeures du gouvernement fédéral. Les compagnies ayant été victimes ne peuvent, dans 33% des cas, identifier l'individu à la source de cette infiltration et que lorsqu'identifié, 77% sont effectivement des employés (Skinner et Fream, 1997). De plus, selon Copes et Vieraitis (2007), 35,5% des individus de leur échantillonnage ont affirmé que leur

emploi créait une opportunité à commettre le délit. Quant à l'étude sur la cybercriminalité effectuée auprès d'entreprises (PriceWaterHouse Coopers, 2013), 35% des crimes les plus dommageables étaient perpétrés par des individus en interne, versus 31% à l'externe et 34% inconnus. Ainsi, ce phénomène n'est pas que prisé par des délinquants inconnus, mais bien aussi par des connaissances et des gens de confiance dans une entreprise. Historiquement, il y a une plus grande proportion d'attaques à l'interne.

En ce qui a trait aux victimes corporatives, selon Hollinger (1991), les délinquants informatiques sont davantage attirés par les grosses entreprises ou compagnies, plutôt que les individus ou les petites firmes. À préciser que 25 ans plus tard, nous ne disposons que de très peu d'études qui nous permettent de penser que la situation a beaucoup changé, ce qui rend donc pertinente l'analyse de la motivation des pirates. Selon le CSI Computer Crime and Security Survey de 2010-2011 (Richardons, 2011), 41,1% des entreprises auront expérimenté un incident informatique. Il est possible d'émettre l'hypothèse que les délinquants ciblant des entreprises de grande envergure visent un objectif plus élevé, comme un profit considérable qu'ils ne retrouveraient pas en attaquant de petites firmes ou des individus ou bien, puisqu'il y a plus d'employés dans de plus grandes entreprises, le risque d'être victime se trouve augmenté. Le tout sera confirmé dans le cadre de la présente étude. Quant aux agences gouvernementales, la moitié aurait déjà été victime d'infiltration et de problèmes relatifs à la sécurité, tout comme 100% de celles-ci ont déjà expérimenté des problèmes de nature criminelle quant à leurs sites Internet (Leeson et Coyne, 2005; Telus-Rotman, 2013). ;

Au niveau du rapport de Norton (2011), des statistiques sont relevées quant aux individus les plus à risque d'être victimes de cybercriminalité. Pour ce qui est de la provenance et l'origine des victimes, il est mentionné que 80% des adultes de pays émergents seront victimes de cybercriminalité, comparés à 64% des adultes venant de pays développés. Cette statistique peut s'expliquer par un manque d'outils et de moyens de prévention dans les pays encore en développement.

Maintenant, il est pertinent de se pencher un peu plus sur l'aspect légal de cette criminalité, soit au niveau des plaintes, des poursuites et des procédures judiciaires. D'abord, dans 96% des cas de crimes informatiques, les victimes ne portent pas plainte, ce qui est une proportion considérable confirmant une sous-déclaration de ce type de criminalité (Verizon, 2012). Quant au CSI Computer Crime and Security Survey de 2010-2011 (Richardson, 2011), seulement 27% des entreprises ont rapporté le délit aux autorités, ne croyant d'abord pas que les autorités pourraient aider, jugeant l'incident de trop faible gravité ou ne voulant pas prendre le risque que cette mauvaise publicité ait un impact sur l'organisation. Les compagnies sont effectivement réfractaires à l'idée de rapporter le délit dû au manque de confidentialité ainsi que la honte que cela risquerait de créer en démontrant une telle vulnérabilité dans leurs logiciels et sites Internet (Young, Zhang et Prybutok, 2007; Leeson et Coyne, 2005; Wall, 2009). De plus, «cette sous-déclaration s'explique par le manque de sensibilisation à ces infractions et la méconnaissance des mécanismes de déclaration, la honte et l'embarras des victimes, et, dans le cas des entreprises, la crainte de voir leur réputation compromise» (UNODC, 2013). Dans l'étude des États-Unis sur la cybercriminalité (PriceWaterHouse Coopers, 2013), un sondage fut effectué auprès de 500 experts en sécurité, dirigeants américains et autres individus en provenance de secteurs publics et privés et ayant

donné leur point de vue quant à l'état de la cybercriminalité. Ils furent questionnés afin de savoir s'ils avaient un plan de politiques et procédures à appliquer dans le cas où un évènement de cybercriminalité se produirait à l'encontre de leur organisation. Seulement 26% des organisations recensées ont répondu qu'elles avaient un plan testé au moins une fois par année. Quant aux entreprises ayant un plan, non testé, elles représentent 26% de l'échantillon. Pour les 48% autres organisations, elles ne savaient pas si elles avaient des procédures (19%), n'avaient pas de procédures, mais prévoyaient en établir dans la prochaine année (17%) ou tout simplement n'en avait pas et il n'était pas dans leurs intentions d'en créer (12%). Or, ces statistiques soutiennent le peu d'importance qu'accordent les entreprises à l'ampleur que peut prendre la cybercriminalité. Il est possible que cette caractéristique se rattache aux statistiques susmentionnées, à l'effet que les cybercriminels sont plus enclins à viser les grandes entreprises, de par le fait qu'elles soient mal protégées ou n'interviennent pas si un incident se produit.

Non seulement les délits sont rarement rapportés, mais lorsqu'il y a plainte, dans la majorité des cas, il y aura abandon de la poursuite des procédures judiciaires pour des raisons telles que: ou le suspect n'est pas identifiable, ou bien il en est à son premier délit et qu'il n'est pas jugé nécessaire de le condamner ou même parce qu'il y a possibilité d'effectuer une entente à l'amiable entre les parties (Hollinger, 1991). Ainsi, rares sont les cyberdélinquants pour lesquels des procédures judiciaires seront entamées et lorsqu'initiées, elles sont perçues comme ayant une moindre gravité que les délits dans le monde réel (Hollinger, 1991; Smith, Grabosky et Urbas, 2008). De plus, selon Anderson et coll. (2012), le fait que les délinquants qui commettent les délits se trouvent généralement dans différentes juridictions aura un effet réducteur sur la motivation à

mener les procédures judiciaires ainsi que les chances que les policiers prennent action. En réponse à cette vue d'ensemble, quoique plutôt brève, il est pertinent de se tourner vers le profil des communautés et les caractéristiques sociales de la cyberdélinquance.

1.2 PROFIL DES COMMUNAUTÉS ET CARACTÉRISTIQUES SOCIALES

Au niveau des caractéristiques sociales, il est avant tout possible d'aborder le thème d'une communauté virtuelle de délinquants informatiques puisqu'ils forment une communauté à part entière, et ce, plus précisément dans un environnement en ligne (Jordan et Taylor, 1998; Holt et Kilger; 2008). Cette communauté comprend tous les moyens mis à leur disposition afin de communiquer et d'être en relation. Ces nombreuses ressources à leur disposition vont faciliter les actes délinquants, donc favoriser une sous-culture délinquante. Selon Chiesa, Ciappi et Ducci, 2008, les délinquants faisant partie de cette communauté sont très liés, ce qui fait en sorte qu'il est difficile pour un jeune pirate d'y pénétrer. Ils se doivent de prouver et démontrer qu'ils ont le potentiel nécessaire pour intégrer la communauté et qu'ils ne sont pas dangereux (Chiesa, Ciappi et Ducci, 2008). Cette communauté, aidée par les plateformes informatiques, recrute de nouveaux pirates, crée des réseaux de communication pour partager des connaissances et s'organise stratégiquement pour former rapidement de bonnes habiletés informatiques (Beveren, 2001; Meyer, 1989). Le partage d'information est un aspect important pour ces pirates (Chiesa, Ciappi et Ducci, 2008). En effet, toujours selon ces auteurs, pour ces passionnés d'informatique, l'apparence, le pouvoir ou le statut socioéconomique qu'ils occupent n'est pas ce à quoi ils porteront attention, mais bien les habiletés qu'ils ont développées ainsi que l'entraide qui permettra de cheminer davantage au niveau de leurs capacités et connaissances (Jordan et Taylor, 1998).

Certaines propriétés sont spécifiques à ces groupes de pirates, notamment le secret et l'anonymat (Jordan et Taylor, 1998; Jordan, 2008). L'aspect secret est en fait l'ambivalence que vivent les professionnels de l'informatique entre le partage d'information dans le groupe, ainsi que le caractère illégal de ce partage. Ils commettent des actes de piraterie afin d'avoir de la reconnaissance des pairs délinquants, mais veulent en même temps ne pas être reconnus par le grand public afin d'éviter toute arrestation. Ceci nous mène à l'anonymat, où les cybercriminels peuvent aisément créer plusieurs identités en ligne (Holt et Kilger, 2008; Leeson et Coyne, 2005; Nissenbaum, 2004; Holt, 2009). Les pseudonymes qu'apposent les délinquants sont des plus importants, tout comme leur désir de demeurer dans la discrétion. Dans le domaine de la cybercriminalité, les crimes ou le réseautage sont souvent effectués dans un contexte d'anonymat. C'est en fait une caractéristique sociale importante de la cybercriminalité, ayant un impact dans le peu de dénonciation des délinquants, tout comme l'amoindrissement des probabilités d'arrestations. C'est un aspect prédominant chez les cybercriminels, dépeints par l'utilisation de surnoms afin de se représenter (Holt et Kilger, 2008; Leeson et Coyne, 2005; Nissenbaum, 2004; Holt, 2009; Padhye et Gujar, 2012). Généralement, ils portent une identité lorsqu'ils naviguent dans les réseaux informatiques, une autre pour naviguer sur Internet ainsi qu'une dans la vie réelle, n'étant jamais révélée à la population appartenant au monde virtuel. Effectivement, l'un des règlements des forums consiste à changer de nom d'utilisateur d'une plateforme à l'autre (Holt, 2009). Il est rare que le nom d'un cyberdélinquant soit utilisé dans toutes ses démarches informatiques, sauf dans le cas où le sujet est arrêté ou qu'il désire exhiber ses connaissances et ses habiletés à la population (Holt, 2009). Ces multiples surnoms leur permettent de se dissocier de la réalité, de vivre une double vie s'ils désirent s'engager dans des comportements marginaux tout en continuant leur rythme de vie habituel, et ce, dans des moments où des évènements et situations personnelles les font sentir plus vulnérables

(Auray et Kaminsky, 2006). D'ailleurs, selon Jordan et Taylor (1998), ils prennent du temps pour sélectionner leurs pseudonymes avec soin.

Selon Holt et Kilger (2008), il existe deux types de communautés de pirates informatiques. Ceux qui sont dans un environnement bien contrôlé, soit au niveau des restrictions scolaires ou familiales, et ceux vivant dans un environnement incontrôlé, donc où aucun encadrement ou support n'est réellement présent. D'abord, ceux vivant dans un environnement contrôlé ont moins de chance d'avoir des amis qui seront cyberdélinquants et communiqueront moins en ligne. Donc, ils ne feraient pas partie de cette communauté. Quant à ceux dans un environnement non contrôlé, ils utiliseront davantage les réseaux de communications et feront partie de la communauté. C'est ici que la théorie de l'apprentissage social entre en jeu, où les cybercriminels dans un environnement non contrôlé s'associeront avec des pairs supportant leurs comportements, des délinquants qui vont donc, comme eux, commettre des actes cybercriminels. Ils vont ainsi justifier et rationaliser leurs comportements parce qu'il est acceptable de le faire au sein de leur communauté. Plus ils seront en contact avec celle-ci, plus il y aura de chance qu'ils imitent leurs comportements et qu'ils adoptent des comportements délinquants (Rogers, 2010).

En ce qui a trait à l'organisation des communautés, il est possible de relever quatre caractéristiques (Best et Luckenbill, 1994) : 1) il peut y avoir une association entre les délinquants, 2) les cybercriminels peuvent participer dans des comportements déviants seuls ou en groupe, 3) il est possible qu'il y ait une division des tâches dans le groupe et finalement, 4) il peut y avoir persistance des comportements à travers le temps et l'espace. De plus, il y a cinq formes d'organisations déviantes, soit : les solitaires (où aucune des caractéristiques n'est appliquée), les collègues (où

uniquement l'association mutuelle est présente), les pairs (où il y a présence de l'association mutuelle ainsi que de la participation mutuelle), l'équipe (étant comme les pairs, mais avec la division des tâches) et l'organisation formelle (regroupant les quatre caractéristiques). L'auteur (Holt, 2009) conclut que les pirates se situent en fait dans la catégorisation des pairs de Best et Luckenbill (1994), bien que ces derniers agissent dans 70% des cas seuls. Ici, l'auteur s'est fié à la catégorisation de Best et Luckenbill (1994), lesquels soutenaient que les délinquants peuvent s'organiser de manière différente, et ce, en fonction du temps et des sociétés. Il est donc intéressant de voir que le pays d'origine du délinquant a possiblement une influence au niveau de l'aspect solitaire ou non de la cyberdélinquance, mais l'auteur n'a pas davantage approfondi cet aspect, ce que l'étude actuelle tentera de faire.

Selon Verizon (2012), dans 70% des cas les pirates ont agi seuls, laissant ainsi croire que la cybercriminalité ne se commet pas en groupe. Bien qu'ils commettent leurs actes seuls, ils demeurent bien entourés grâce aux forums et aux réseaux sociaux, permettant de nombreux échanges et un support mutuel avec les autres amateurs d'informatique (Meyer, 1989). En effet, afin de combler cette solitude et ce manque de support relationnel, les délinquants vont rechercher des ressources virtuelles (Holt et Kilger, 2008).

Également, selon Holt (2009), 76% des cybercriminels fréquentent des pairs qui sont eux aussi attirés par les délits informatiques. Certains seront affiliés à des groupes de cybercriminels, par exemple Anonymous, Lulzsec, etc. Plus précisément, Anonymous est un mouvement mondial composé d'«hacktivistes» qui revendiquent la liberté d'expression en faisant usage de leurs habiletés et technique informatique. Ils tentent de faire passer leur message avec un mode d'action non

violent, soit la piraterie informatique, en s'attaquant aux grandes multinationales et aux gouvernements. Ce groupe est très anonyme et il n'est pas possible de chiffrer le nombre de cyberdélinquants y étant affiliés. Ils défendent «la liberté d'expression, le pouvoir du peuple, le droit de manifester contre les gouvernements, de rendre justice » (Saumet, 2015). Quant au groupe Lulzsec, c'est aussi un mouvement composé de délinquants informatiques, dont certains venaient du groupe Anonymous, et qui agissent en attaquant aussi des multinationales ou gouvernements. Toutefois, dans leur cas, ce sont des «hacktivistes» motivés par la notoriété engendrée par le délit. Il est intéressant de soulever que ce groupe fut éphémère. Effectivement, des arrestations massives furent effectuées suite à leurs comportements (Cheng et Reisinger, 2012; Cluley; 2011). Bref, malgré que la majorité des cyberdélinquants commettent leur délit sans aucun complice, il n'en demeure pas moins qu'ils ont un entourage ayant les mêmes motifs et objectifs qu'eux ou qu'il y a des chances qu'ils soient affiliés à un groupe de pirates informatiques, ce qui les encouragent et les maintiennent dans un mode de vie marginal.

1.3 LE PROFIL DES CYBERCRIMINELS

Maintenant que la vue d'ensemble du phénomène de la cybercriminalité est achevée, il est intéressant de se pencher sur le type de délinquant se cachant derrière celle-ci. Ainsi, cette sous-section brossera son portrait, en abordant les différentes caractéristiques démographiques des délinquants, leurs motivations, leur degré de compétence ainsi que les caractéristiques psychologiques de ces derniers. Également, une section sera attribuée pour l'identification des divers profils étudiés.

1.3.1. Profil de l'individu

Qui sont ces cybercriminels cachés derrière un ordinateur et commettant des délits dans un monde parallèle? Quelle image la société s'est-elle créée de ceux-ci? Il semble qu'ils soient peu connus de la société et que des images erronées se soient fondées au fil des années de par un manque de connaissance. Afin de remédier à celles-ci, voici pour commencer les caractéristiques démographiques de ces cyberdélinquants.

1.3.1.1 Caractéristiques démographiques

Des stéréotypes se sont bâtis au fil des années, emmenant la population à généraliser ce type de délits ainsi que le profil du cyberdélinquant lui-même. Il est souvent perçu comme un personnage sombre, ne prenant pas soin de son apparence et très antisocial, ayant des aptitudes sociales défaillantes ou provenant de familles dysfonctionnelles (Rogers, 2006; Lusthaus, 2012). Effectivement, selon Rogers (2006), la population visualise des adolescents âgés de 14 et 18 ans. De plus, ce sont à leurs yeux des individus travaillant uniquement de nuit. L'image du jeune surdoué devant son ordinateur est aussi un cliché populaire, avec les grosses lunettes, la peau pâle et une coupe de cheveux laissant à désirer (Jordan, 2008; Koops, 2011; Wori, 2014). La déficience d'études approfondies au niveau de la cybercriminalité est en partie la cause de telles créations de stéréotypes. Par ailleurs, les médias jouent un rôle important dans la formation de ces stéréotypes en rapportant les histoires les plus typiques et alléchantes pouvant intéresser le public, tout comme les documentaires et les films hollywoodiens fortement caricaturaux (Nissenbaum, 2004; Rogers, 2006; Simon, 2005; Taylor, 1999; Woo, 2003). Ils construisent ainsi des modèles n'étant pas réellement issus de profils physiques, psychologiques, socioéconomiques et démographiques concrets des cybercriminels, formant par conséquent des généralisations fautives nuisant aux futures recherches.

Afin de démystifier le tout, voici d'abord les caractéristiques démographiques du profil type du cybercriminel. Celles-ci sont semblables d'une étude à l'autre. D'abord, il est souvent énoncé que les cybercriminels sont majoritairement des hommes (Jordan et Taylor, 1998; Dupont, 2012; Woo, 2003; Schell, 2007; Moon, McCluskey et McCluskey, 2010; Jordan, 2008). Ce constat est aussi supporté par l'étude de Taylor (1999), où le ratio des cybercriminels est de 99 hommes pour une femme (Yar, 2005). Ce crime est donc, à commun accord, à forte prévalence masculine.

En ce qui a trait à l'âge type des cybercriminels, il serait en moyenne de 18 ans (Holt et Schell, 2011). En effet, le portrait de ces individus se situe couramment en bas de la mi-vingtaine, tout comme le supporte Hollinger (1991). La précocité dans l'agir délinquant est aussi un élément important à mentionner dans le cas des cybercriminels. L'âge moyen de la naissance des intérêts envers les technologies et la complexité de celle-ci est évalué entre 8 à 11 ans (Dupont, 2012; Holt et Schell, 2011; Auray et Kaminsky, 2006). De plus, il fut établi dans l'étude de Chiesa, Ciappi et Ducci (2007) qu'il y a beaucoup de jeunes qui débutent dans la tranche d'âge de 11-12 ans, que la plupart des intéressés d'informatique amorcent leur criminalité dans la tranche d'âge de 13-14 ans, et qu'une minorité l'entreprendrait entre 18 et 19 ans. Il est donc possible d'observer une constance quant à la précocité des actions délinquantes.

Yar (2005) explique cette manifestation hâtive comme une conséquence des facteurs psychologiques chez l'enfant ou l'adolescent. L'individu passe inévitablement par certaines phases d'apprentissage, dont celui de la maturité. Lorsqu'il est jeune, il n'est pas suffisamment mature pour bien gérer son degré d'impulsivité et n'a pas encore assez de moralité pour comprendre jusqu'où il

peut aller. L'âge moyen de désistement de ces individus dans leurs comportements criminels est dans le début de la vingtaine, là où la maturité commence tranquillement à s'acquérir. De plus, Auray et Kaminsky (2006) soutiennent que l'agir n'est pas uniquement basé sur le choix de l'enfant, mais qu'il est aussi en partie une conséquence du choix parental. Évidemment, il est possible d'émettre l'hypothèse que les parents vivent un certain manque de connaissance quant aux possibilités offertes par les nouvelles technologies, et ce, particulièrement en terme de délinquance. Il a été démontré que dans plusieurs cas, le pirate ayant commencé dès un jeune âge avait reçu l'ordinateur en cadeau de la part de ses parents, n'en ayant pas restreint l'usage bien qu'il soit abusif. Bref, cette hypothèse est une piste intéressante, mais qui demeure sujette à approfondissements. Pour faire suite à ce rapide survol du profil du cyberdélinquant, il est approprié de se pencher sur la motivation du cyberdélinquant à commettre ses délits.

1.3.1.2 Les motivations du délinquant

De jeunes hommes seront plus enclins à commettre des délits informatiques, certains appartiendront à des groupes, d'autres seront plus solitaires. Mais dans les faits, il est intéressant d'étudier aussi les motivations de ces derniers à s'impliquer dans de tels délits, leur degré de compétence ainsi que leurs caractéristiques psychologiques afin d'avoir un meilleur portrait du profil de ces pirates.

Pour que le crime soit possible, divers facteurs doivent être présents, notamment le facteur motivationnel du cyberdélinquant. La motivation est l'élément principal à la base de ces occasions criminelles (Cohen et Felson, 1979) et est jugée comme étant un élément discriminatoire très utile pour comprendre la cybercriminalité (Jordan, 2008). Effectivement,

s'il n'y avait pas un mobile poussant un délinquant à agir, la criminalité n'existerait pas. La motivation est donc le maillon initial de la chaîne délictuelle. Évidemment, deux sources de motivations existent, soit les motivations intrinsèques et extrinsèques (Lakhani et WOQLF, 2005; Deci et Ryan, 2000). La motivation intrinsèque est reliée à la notion du plaisir que retire l'individu à agir tout comme l'obligation qu'il ressent à le faire pour sa communauté. La motivation extrinsèque, elle, comprend les récompenses que retire l'individu suite à l'action, tel un gain financier.

Diverses motivations sont à l'origine de la cybercriminalité et de nombreuses typologies ont été établies par plusieurs auteurs. Voici d'abord un regroupement des motivations les plus communes pour les pirates informatiques: dépendance à l'adrénaline, curiosité (exploration), vie hors-ligne monotone, augmentation du pouvoir, reconnaissance des pairs, complexe de Robin des Bois, soit rendre service de par leur générosité, l'argent, le désir de protestation, l'esprit de jeu, la fierté, l'ingéniosité (innovation) ainsi qu'une rancune ou une offense personnelle (Jordan et Taylor, 1998; Chiesa, Ciappi et Ducci, 2007; Verizon, 2012; Simon, 2005; Jordan, 2008).

Une autre motivation est soulevée, différente de celles qui sont susmentionnées, incluant davantage la notion du libéralisme, soit la voie politique (Jordan, 2008). Ces délinquants sont surnommés les «hacktivistes». Ils commettent de tels actes uniquement dans le but d'avoir une voix et de protester en faveur de leur liberté et du droit à l'information. Ces délinquants perçoivent leur crime comme un moyen d'avoir une liberté de parole, une vie

privée, une certaine individualité ainsi que de la méritocratie. Leur criminalité est selon eux un moyen d'expression (Coleman et Golub, 2008).

Quelques statistiques intéressantes permettent d'établir un ordre de priorité au niveau des motivations des pirates informatiques (Holt et Schell, 2010). L'échantillon (N=124) fut colligé par des sondages autorapportés, distribués lors d'une grande convention de « hackers » à Washington en février 2008. La motivation la plus commune est la curiosité, soit 95% de leur échantillon. Viennent ensuite l'expérimentation (85%), le plaisir et l'amusement (66%), le pouvoir procuré par le crime (21%) et finalement, le besoin de reconnaissance des pairs (19%). Seulement 10% de leur échantillonnage a répondu la revanche comme motivation. Dans cette étude, aucun résultat n'est obtenu par rapport à la motivation financière, soit d'obtenir du profit de la criminalité.

Ensuite, il existe différents types de délinquants, ayant conséquemment des sources de motivation distinctes (Leeson et Coyne, 2005; Holt et Kilger, 2008). D'abord, les «bons pirates», «white hat» ou «Elite» sont ceux agissant par bonne volonté, soit plus précisément ceux qui désirent faire avancer les connaissances et les capacités informatiques ainsi qu'améliorer la société (Turgeman-Goldschmidt, 2008; Chandler, 1996). Ils se servent de leurs habiletés informatiques comme un outil à la disposition de la société afin de faire avancer les choses, sans causer de torts à qui que ce soit. Ensuite, il y a les «pirates malveillants», «black hat», lesquels ont des motivations instrumentales et n'ont qu'un désir de pouvoir ou de célébrité. Sont rangés par exemple dans cette catégorie les pirates qui volent la propriété intellectuelle d'entreprises ou qui développent des logiciels malveillants. Ce sont eux qui

créent des dommages chez les victimes et qui coûtent cher à la société. Ils sont mésadaptés socialement et recherchent la reconnaissance des pairs (Leeson et Coyne, 2005; Turgeman-Goldschmidt, 2008; Jordan, 2008). Aussi, ils ressentent un certain désir de vengeance, de destruction et de vandaliser certains sites Internet. Ils sont aussi surnommés les «crackers», les «losers» et les «darksiders» (Goodell, 1996; Chandler, 1996; Adamiski, 1999). Dans cette catégorie peuvent aussi être inclus les «hackers» avares ou «grey hat», soit ceux qui commettent des délits dans le but d'obtenir des profits, peu importe le moyen qu'ils devront prendre pour arriver à leurs fins. Ils sont partagés entre le côté sombre («black hat») et le côté éclairé («white hat») de la cybercriminalité. Le but ultime est d'obtenir un profit au bout de leurs actes, soit en travaillant pour la sécurité, soit en faisant de la fraude. Il est donc possible de détecter une ambivalence dans la motivation de ces délinquants, selon la considération qu'ils auront d'autrui.

Il est aussi intéressant de se pencher sur la typologie des auteurs de crimes informatiques afin de dégager divers profils motivationnels. Comme le but de l'étude actuelle est de vérifier s'il existe des différences de profils à l'échelle internationale, il est intéressant de soulever les taxonomies déjà existantes. Il est énoncé dans l'étude de Howard (1997), qui brossera un aperçu des différents profils des auteurs de crimes informatiques ainsi que les motivations les amenant à commettre des délits informatiques, six (6) types de pirates. D'abord, il y a le «hacker», plus précisément le pirate informatique qui infiltre des ordinateurs, et ce, pour relever le défi d'obtenir un accès illégal. Est ensuite identifié l'espion, soit le pirate informatique qui s'infiltre dans les ordinateurs afin d'acquérir de l'information qui sera utilisée dans l'optique d'obtenir un profit politique. De plus, le terroriste est l'un des pirates informatiques qui sont inclus dans la typologie. Il s'agit du pirate qui infiltre les

ordinateurs pour instaurer la peur, et ce, également dans un but politique. Quant au prédateur entrepreneur ou «Corporate Raider», il s'agit d'un employé d'une compagnie qui infiltre les ordinateurs de l'entreprise en compétition à la leur, et ce, dans le but d'obtenir un gain financier. Également, l'auteur identifie le criminel professionnel qui pénètre les ordinateurs, motivé par un gain financier personnel. Finalement, il y a le vandale, celui qui infiltre les ordinateurs dans le seul objectif de causer des dommages (Howard, 1997, p.63).

Plus simplement, Goodell (1996) a défini les cyberdélinquants comme les «hackers», les «crackers» et les «phreakers». Les «hackers» constituent ceux motivés par la curiosité intellectuelle et le désir d'acquérir de nouveaux apprentissages. Les «crackers» ont un objectif malsain de destruction, de vandalisme de sites Internet et de pages web. Quant aux «phreakers», leurs délits sont dirigés vers la manipulation de systèmes téléphoniques ou vers des attaques de ces derniers.

Une autre typologie englobant neuf (9) catégories de cybercriminels est soulevée dans l'étude de Rogers (2006) et permet d'identifier les motivations générales pour chacun de ces auteurs. Il y a d'abord la catégorie des «novices», lesquels sont motivés par la notoriété que rapporte le crime, le besoin de reconnaissance et le besoin de défi. La catégorie des «cyberpunks» représente ceux qui sont motivés par l'attention procurée par les médias et dans certains cas, le profit gagné de leur criminalité. Ils ciblent des victimes importantes afin de recevoir de l'attention en s'engageant dans une criminalité narquoise. Quant aux «internals», ils représentent d'anciens employés en sécurité informatique ressentant le besoin de se venger, tout en faisant montre de rationalisation en justifiant leurs actes. En ce qui a trait aux « petty thieves», leurs motivations sont plus nombreuses, notamment le profit de la criminalité, l'avidité et parfois la revanche. Toujours selon Rogers (2006),

pour la catégorie des «old guards», ils sont motivés par la curiosité ainsi que par de nouveaux défis intellectuels. Pour ce qui est des «virus writters», cette catégorie peut en fait être incluse dans diverses autres classifications, mais une catégorie à part entière fut tout de même créée et tient compte des pirates qui créent leurs propres virus informatiques. La catégorie des «professionnal criminals» présente les professionnels qui commettront des délits dans un but unique de profit et de gain financier. Les «informations warfare» sont des individus agissants par patriotisme. Finalement, il y a les «political activists», qui inclut la majorité des classifications susmentionnées et qui sont motivés par l'aspect idéologique et politique (Rogers, 2006).

Il est possible d'observer, suite à l'énumération de ces typologies, qu'il existe une grande diversité de profils de cybercriminels. Ces dernières permettent au lecteur d'avoir une meilleure idée des motifs dégagés pour chacun des profils des auteurs de crimes informatiques. Plusieurs autres auteurs ont identifié des catégories de pirates informatiques, notamment Parker (1998), Landreth et Rheingold, (1985), Power (1998), etc. Toutefois, celles qui sont susmentionnées permettent d'établir un portrait général et englobant ces diverses classifications. Comme la motivation divergera d'un individu à l'autre, entrera en jeu le degré de compétence de ces derniers puisqu'il aura certainement un impact sur le type de criminalité utilisée.

1.3.1.3 Le degré de compétence technique du délinquant

Avant même de plonger dans la recension du degré de compétence des délinquants, il est bon de prendre connaissance des différentes habiletés qu'ils doivent détenir afin d'être reconnus comme des cybercriminels (Copes et Vieraitis, 2007). Il s'agit en fait d'un cadre théorique formulé dans le contexte du vol d'identité, mais qui peut très bien être transféré au

piratage informatique. Ces différentes habiletés sont élaborées à quatre niveaux, soit celles de la sphère sociale, la sphère technique, la sphère intuitive et finalement, la sphère des connaissances. Les habiletés techniques comportent le savoir-faire quant à la production de documents falsifiés, volés et frauduleux. Ce niveau d'habileté est nécessaire dans le monde de la piraterie informatique étant donné que ce sont ces dernières qui permettront aux pirates d'arriver à leurs fins, de commettre le délit qu'ils désirent et de faire du profit, pour ceux attirés par l'aspect financier. Effectivement, avec un manque d'habiletés techniques, ils ne parviendront pas à atteindre leurs objectifs (Copes et Vieraitis, 2007; Dupont, 2012). En ce qui a trait à la sphère des habiletés sociales, il est question de leur agilité à manipuler l'individu. Non seulement il y a ce caractère manipulatoire, mais cette habileté est aussi applicable chez les cybercriminels dans le sens où ils doivent construire des liens de confiance avec d'autres pirates qu'ils n'auront fort probablement jamais vus de leur vie. Ils doivent apprendre à tisser ces liens et à les maintenir, afin de s'entraider dans les trajectoires les amenant vers le délit. S'ils ont besoin de renseignements, qu'une tâche soit effectuée, mais que leurs habiletés techniques sont déficientes et que c'est le seul moyen d'atteindre leur objectif délictuel, bref, advenant qu'ils aient besoin d'aide, leur réseau social de confiance sera leur support et leur permettra de partager de multiples informations afin atteindre leur but. Ainsi, les pirates ayant la capacité de générer et de conserver un réseau social de qualité ont de meilleures chances au niveau des occasions criminelles. Dans le sens inverse, les pirates ayant un faible réseau social ainsi que des relations où la confiance n'est pas présente sont à risque d'avoir un moins bon rendement. Ces pirates prendront moins de risques donc, seront moins innovateurs et finalement, il y aura une réduction des profits qu'ils pourraient retirer de leur criminalité. Cette instabilité que les cyberdélinquants vivront, ainsi que la contrainte qu'ils subissent au niveau

du manque de confiance aura pour effet de nuire à leurs relations (Copes et Vieraitis, 2007; Dupont, 2012). Ensuite, leurs connaissances des systèmes se doivent d'être accrues. En effet, ils doivent bien connaître la manière dont les systèmes et les réseaux sont opérés afin de pouvoir s'y infiltrer (Copes et Vieraitis, 2007). Non seulement ils doivent avoir un haut degré de connaissance, mais ils doivent aussi savoir quels sont les marchés noirs sur Internet, comment faire des échanges de produits volés, avoir des connaissances des alternatives au niveau de la vente sur le marché noir et même savoir avec qui il est sécuritaire de faire affaire (Dupont, 2012). D'ailleurs, cela nous mène sur le plan des habiletés intuitives, lesquelles sont en lien avec la sensibilisation quant aux risques de se faire prendre par les autorités (Copes et Vieraitis, 2007).

Cela dit, voici les divers degrés d'habiletés techniques en fonction de la typologie énumérée dans la section des motivations des cybercriminels, soit celle de Rogers (2006). Les «novices» sont plus jeunes et présentent des techniques de programmation et des habiletés informatiques limitées. La catégorie des «cyberpunks» représente ceux qui ont davantage d'habiletés informatiques et une meilleure compréhension des systèmes d'attaques informatiques. Quant aux «internals», ils représentent d'anciens employés en sécurité informatique, donc qui ont déjà des habiletés techniques avancées. En ce qui a trait aux « petty thieves», ils font l'apprentissage des techniques préalables à la commission de leur acte délictuel puisque leurs cibles traditionnelles ont migré vers le monde virtuel. Or, leurs habiletés sont limitées. Ensuite, pour la catégorie des «old guards», ils possèdent des habiletés technologiques avancées et créeront parfois eux-mêmes le virus ou le logiciel malicieux à l'origine de l'attaque informatique. Pour ce qui est des «virus writters», il s'agit des pirates qui créent leurs propres virus informatiques, ce qui représente un degré d'habiletés techniques somme

toute avancé (Rogers, 2006). La catégorie des « professionnal criminals» présente les professionnels qui commettront des délits pour leur entreprise et qui ont une intuition criminelle et des habiletés techniques avancées. Les «informations warfare» sont en fait des individus entrainés, ayant des habiletés très développées et qui ont comme mission la défense contre les attaques externes. Cette catégorie, ainsi que celle des «professionnal criminals» représente les groupes les plus dangereux et qui ont développé des spécialités en matière de criminalité informatique. Ils ont l'équipement avancé leur permettant d'agir et sont très bien entraînés. Finalement, il y a les « political activists», qui inclut la majorité des classifications susmentionnées (Rogers, 2006).

Toutefois, certaines typologies sont plus globales, telle la typologie de l'étude de Young, Zhang et Prybutok (2007), où ils identifient uniquement deux catégories, ainsi que celles de Chantler (1996) et de Hollinger (1988), incluant toutes deux trois catégories. Young, Zhang et Prybutok (2007) identifient d'abord les «hackers élite», soit les pirates informatiques présentant un degré d'innovation élevé et qui ont une connaissance avancée des systèmes informatiques. Ils présentent ensuite les «kiddies», soit ceux qui font usage d'outils déjà mis à leur disposition afin d'infiltrer et d'attaquer les systèmes informatiques (Young, Zhang et Prybutok, 2007). Quant à Hollinger (1988) et Chantler (1996), les catégories sont similaires. Hollinger (1988) identifie les catégories suivantes : «pirates, browsers, and crackers». Chantler (1996) énumère les groupes suivants : «elite, neophytes, and losers». D'abord, les «pirates» et «loosers» sont ceux ayant un faible degré de compétences techniques limitées au piratage des logiciels informatiques. Quant aux «browsers» et «neophytes», ils représentent un niveau d'habiletés techniques modéré et présentent les connaissances nécessaires pour infiltrer des fichiers personnels d'individus. Ils sont en apprentissage continu et leur but n'est pas de créer des dommages dans ces dossiers, mais plutôt de les infiltrer. En ce qui a trait aux

«crackers» ou «elite», ce sont les catégories qui incluent le niveau d'habiletés techniques le plus élevé. Elles représentent en fait les cyberdélinquants les plus sérieux.

Maintenant que les habiletés des cyberdélinquants ont été mentionnées, explorons le degré de compétence de ces derniers. Il est qualifié soit de très faible, de faible, de modéré ou d'élevé (Verizon, 2012). Une limite est identifiée dans cette étude, soit qu'il y a un certain degré de subjectivité dans la classification. Somme toute, cette échelle sera un bon indicateur du niveau d'effort apporté par le cyberdélinquant afin de commettre le délit. Or, selon le niveau de difficulté de ces infiltrations, 4% avaient un niveau de difficulté élevé, 39% présentaient un degré d'efforts apportés modéré, 49% étaient de faible degré et finalement, 2% affichaient un degré de difficulté très faible (Verizon, 2012). Il est possible de constater que rares sont les infiltrations informatiques générées par des individus ayant un très haut niveau de compétence et que celles perpétrées par des individus ayant un très faible degré de compétence le sont encore plus. Afin de compléter le survol du profil du délinquant, il ne reste que les caractéristiques psychologiques à explorer.

1.3.1.4 Aspect psychologique du cyberdélinquant

Comme plusieurs profils psychologiques de la délinquance ont déjà été étudiés, celui des cybercriminels fut également établi dans quelques études (Chiesa, Ciappi et Ducci, 2007; Schell et Dodge, 2002). Diverses caractéristiques psychologiques y sont énumérées, et ce, afin de mieux pouvoir saisir la personnalité de ces délinquants informatiques. D'abord, il est mentionné dans l'étude de Woo (2003) qu'ils ont un profil de manipulateur, arrogant, et qui relève du narcissisme. Ces propos semblent généralisateurs et doivent être pris sous toute réserve, mais des questionnaires

ont tout de même été distribués sur un échantillon plutôt significatif et ceux invalides furent supprimés de leur liste. L'étude a été menée auprès de 1 385 pirates informatiques, provenant de trente (30) différents pays et ayant participé à un sondage en ligne. Comme les pirates informatiques ne sont pas connus de la population de par leur anonymat, le questionnaire (68 questions) fut distribué sur le site «free hacking zone» et l'équipe gérant ce site a veillé à le protéger des pirates malicieux. Les critères de sélection des questionnaires ont été établis selon deux règles. D'abord, il devait être rempli à plus de 70% et si le répondant semblait répondre sans sérieux, notamment en sélectionnant les mêmes choix de réponses d'une question à l'autre, il n'était pas pris en compte. De plus, si le pirate informatique ne répondait pas aux questions cibles préalablement sélectionnées par les chercheurs, le questionnaire était automatiquement éliminé. À la fin du processus, 729 questionnaires étaient valides. Bref, cette étude maintient que les cyberdélinquants ont une perception d'eux-mêmes peu modeste (Woo, 2003). Effectivement, ils se perçoivent comme des personnes extraordinaires. Ils affirment avoir un niveau d'intelligence supérieure au reste du monde et affichent une certaine attitude de supériorité et de pouvoir. Ils se perçoivent comme importants dans l'actualisation et dans le changement de la société (Turgeman-GOQLFschmidt, 2008).

Ensuite, certains criminels vivent des difficultés au niveau psychophysique (Chiesa, Ciappi et Ducci, 2007). Sur un échantillon de 216 cyberdélinquants, certains ont tendance à faire de l'insomnie (34%). Afin d'avoir un comparatif quant à la population ordinaire, une étude effectuée au Québec, dans laquelle 2001 adultes francophones ont répondu à une enquête téléphonique, allègue que 29,9% de la population présente des symptômes d'insomnie (Leblanc, 2006). Sur un échantillon supérieur, le résultat des cyberdélinquants faisant de l'insomnie est plus élevé, donc il est

possible d'observer que la prévalence d'insomnie chez les cyberdélinquants est plus importante que dans la population ordinaire. De plus, 6% des pirates hallucinent (Chiesa, Ciappi et Ducci, 2007), ce qui est plus important que la prévalence des cas dans la population ordinaire, où suite à une étude téléphonique menée auprès de la population normale au Royaume-Uni, en Allemagne et en Italie (N=13 057), il fut identifié que 0,5% à 3% des cas ont déjà vécu des hallucinations (Ohayon, 2000). D'autres pirates informatiques seront en dépression majeure et finalement, certains souffrent du syndrome d'Asperger (Wori, 2014).

Ensuite, Chiesa, Ciappi et Ducci (2007) révèlent que les pirates informatiques ont un profil paranoïde et vivent dans l'insécurité. Toujours selon eux, certains de ces délinquants ont des personnalités multiples se reflétant dans la création de plusieurs surnoms, tout comme la double vie qu'ils mènent, soit celle dans la virtualité comparée à celle dans la réalité.

Selon Chiesa, Ciappi et Ducci (2008), au niveau social, soit dans la vie hors-ligne, ces amateurs d'informatique ont de faibles relations interpersonnelles. De plus, ces individus ressentent le besoin d'être reconnus par leurs pairs (Chiesa, Ciappi et Ducci, 2007; Coleman et Golub, 2008). En effet, les jeunes délinquants sont très introvertis et préfèrent d'ordre général être seuls. Ils auront ainsi tendance à s'isoler d'autres individus. Non seulement ils ne se sentent pas acceptés de ceux-ci, mais ils ont aussi une part à jouer dans cet isolement. Effectivement, ces fervents de l'informatique ont une obsession pour les défis qu'apporte le monde virtuel. Ils ont une dépendance par rapport aux défis que leur posent les multiples réseaux informatiques, ce qui les rend indifférents quant à leur faible popularité auprès d'autrui (Chiesa, Ciappi et Ducci, 2008).

1.3.1.5 Diversité des profils identifiés

Suite à la lecture des études présentant le cybercriminel, nous avons pu remarquer une certaine constance dans l'identification des typologies de ces derniers. Rares étaient les fois où des typologies différaient largement. Toutefois, dans ces études, comme identifiés dans les sections précédentes, les profils sont dressés en fonction des différentes motivations des délinquants ainsi que de la divergence des degrés de compétence. Ces typologies varient entre deux à neuf profils distincts (Meyer, 1989; Hollinger, 1990; Chiesa, Ciappi et Ducci, 2007; Rogers, 2006; Youang et al, 2007; Leeson et Coyne, 2005), mais sont tout de même similaires d'une étude à l'autre. Pour les types de délits, ils sont plutôt uniformes dans l'ensemble des recherches, les typologies se recoupant d'une étude à l'autre. Ils se résument aux délits d'infiltration, de fraude, notamment d'hameçonnage, de cyberviolence et de cyberpornographie. Toutefois, rappelons qu'aucune de ces recherches n'étudie l'origine du cyberdélinquant afin d'en établir le profil, ce vers quoi nous dirigerons notre étude. Effectivement, nous évaluerons si ces différents profils, basés sur ces typologies, peuvent s'expliquer par le lieu d'origine du cyberdélinquant plutôt que de les créer uniquement avec l'assise de la motivation ou du degré de compétence.

1.4 LITTÉRATURE S'ÉTANT INTÉRESSÉE AU PHÉNOMÈNE DE LA CYBERCRIMINALITÉ

Le facteur explicatif de l'origine géographique a peu été utilisé dans les études passées, sauf une étude notable, soit celle de Verizon (2012). En effet, des statistiques furent établies quant aux infiltrations informatiques en provenance d'une source externe, et ce, en fonction de différentes régions. Cette étude est basée sur 855 évènements d'infiltrations informatiques et 174 millions

de données compromises en 2011. Subséquemment, 67% des agents externes proviennent d'Europe de l'Est, 20% d'Amérique du Nord, 4% d'Europe de l'Ouest, 2% d'Asie de l'Est, 1% d'Afrique, 1% d'Asie du Sud, 2% d'autres régions et 10% de source inconnue. Il est intéressant de comparer ainsi les sources externes d'infiltration à l'échelle mondiale, mais encore est-il qu'il n'y a pas que ce type de cybercrime pour lequel il serait pertinent d'avoir des données statistiques. Effectivement, il serait intéressant d'avoir une vision plus globale quant aux données obtenues à l'échelle internationale, notamment pour les infractions frauduleuses et les attaques informatiques. De plus, il est important de mentionner qu'il y a présence d'un biais de sélection dans cette étude, plus précisément quant au fait qu'ils aient utilisé différents mécanismes d'entrée de données, donc que des erreurs peuvent en avoir découlé.

The Software Alliance (2011) approfondit aussi la comparaison des vols de logiciels installés sur des ordinateurs personnels dans une année, et ce, en fonction des pays. Afin d'y parvenir, ils ont travaillé avec deux entreprises de recherche indépendantes, soient le IDC et Ipsos Affaires publiques afin de recueillir 182 entrées de données quant à l'évaluation d'ordinateurs et de logiciels dans 116 régions. Il en a résulté que le pays où le taux de vol est le plus élevé est le Venezuela, avec 88%. Celui étant le plus faible est les États-Unis, à 19%. D'autre part et en décroissance, la Chine a un taux de vol de 77%, la Russie 63%, le Mexique 57%, la France 37% et le Canada 27%.

Or, aucune autre étude empirique n'a exploré jusqu'à maintenant les différences significatives de la cybercriminalité selon la provenance du cybercriminel, outre celle de Verizon (2012) qui demeure limitée au délit d'infiltrations informatiques. Dans une optique de prévention et

d'intervention, si l'objectif ciblé est que les moyens offerts à la société afin de se protéger d'un tel crime soient adéquats et efficaces, il serait pertinent d'étudier davantage les caractéristiques de la cyberdélinquance. Notamment, il serait intéressant d'étudier les caractéristiques du cybercriminel, de son délit ainsi que des victimes. En effet, dans une perspective de prévention situationnelle, il est impossible de réduire les occasions ou de diminuer les bénéfices que les délinquants souhaitent retirer de leurs crimes si leur motivation n'est pas connue. De nombreuses campagnes de sensibilisation ont été lancées par rapport à la prévention de cette problématique (ONUDC, 2013). De plus, des entreprises ou des individus se protègent et prennent des mesures supplémentaires pour éviter une quelconque victimisation, soit par l'entremise de pare-feu ou d'antivirus. Toutefois, il semble que des moyens et outils de prévention devraient être davantage adaptés au criminel et pouvoir s'appliquer en fonction des diverses caractéristiques de ces derniers. D'ailleurs, les moyens de répression diffèrent d'un territoire à l'autre, ce qui amène à une difficulté supérieure au niveau des sanctions et de la prévention, et ce, puisque ce type de criminalité peut notamment être perpétré outre-mer (ONUDC, 2013). De plus, il n'existe pas réellement de base de données sur des cybercriminels, et les nombreuses tentatives d'arrestations se soldant par des échecs, ou tout simplement le manque d'arrestation ou de déclaration des victimes ont un effet pervers sur la cybercriminalité. Par exemple, il y a augmentation de la confiance des délinquants, tout comme de leur estime au niveau de la commission d'actes délictuels (Kshetri, 2006). Il sera donc pertinent de faire les recherches et analyses nécessaires dans le but de créer une idée globale de leurs motivations, du type de victime ciblé, du type de criminalité privilégié, et ce, dans le but d'ultimement bâtir des outils de protection et des moyens de prévention efficaces.

Afin de justifier la pertinence d'utiliser l'origine géographique comme facteur explicatif de la cybercriminalité, il est intéressant de comparer avec une étude ayant déjà exploré le crime sous plusieurs aspects au plan international, par exemple l'étude sur les homicides de Ouimet (2011). Cet auteur a mentionné dans son étude l'importance des caractéristiques et des facteurs étant attachés à chaque pays dans la commission d'actes délictuels, plus précisément dans son cas, des homicides. Dans ses résultats, trois composantes ont été soulignées : la population, la situation économique ainsi que le système politique. En premier lieu, il a soulevé que le crime est davantage commis par des individus moins âgés. Ainsi, si la population du pays est en bas âge, il y a de fortes chances que le crime y soit plus élevé. Ensuite, toujours selon Ouimet (2011), plus une population est hétérogène, soit composée de différentes ethnies, religions et langues, plus le taux de crime y sera élevé. Pour ce qui est de la situation économique, les pays peu développés sont davantage à risque d'avoir un taux élevé d'homicides, au contraire des pays industrialisés qui ont un bas taux d'homicide (exception faite des États-Unis). Cette différence du taux de criminalité entre les divers pays serait due à l'inégalité de la distribution économique, soit celle des revenus plus précisément. En ce qui a trait au système politique, lorsqu'un pays tend à réduire le degré de coercition, il y a plus de chances que les taux d'homicide augmentent. Ainsi, «l'impunité pourrait expliquer la forte prévalence de l'homicide» (Ouimet, 2011).

D'autre part, des statistiques intéressantes existent quant au vol de logiciel par des criminels, délit se manifestant de façon importante au niveau mondial et pouvant étayer le choix de travailler avec les dimensions géographiques de la cybercriminalité dans l'étude actuelle. En effet, The Software Alliance (2011) fait des analyses de piraterie informatique depuis quelques années, comme la tendance des vols de logiciels par continent, où les statistiques ne varient qu'entre 0% et 1% de

2009 à 2011. Aux fins de la présente étude, les statistiques les plus récentes en provenance des analyses de The Software Alliance seront étudiées, soit celles de 2011. D'abord, pour avoir une vue globale de cette problématique, il est à noter qu'à l'échelle mondiale, 42% des logiciels sont piratés. En Europe de l'Ouest, c'est 32% des logiciels qui le sont, 62% dans la région de l'Europe centrale/est, 58% en Afrique et Moyen-Orient, 60% en Asie du Pacifique, 61% pour l'Amérique latine/sud ainsi que 19% pour l'Amérique du Nord. Une différence marquante est considérée pour l'Amérique du Nord, où les logiciels semblent les moins piratés, suivie de l'Europe de l'Ouest. Cette différence notable est probablement en lien avec les meilleures protections technologiques offertes aux populations d'Amérique du Nord et d'Europe de l'Ouest, et ce, compte tenu du niveau économique plus élevé permettant d'acquérir des outils technologiques et des outils de protection plus développés, comparés aux régions où la technologie n'a pas atteint son apogée en raison d'une économie plus précaire, telle l'Afrique/péninsule Arabique. Elle peut également être en lien avec les poursuites judiciaires ainsi que les législations plus sévères qui diffèrent d'un pays à l'autre. Toutefois, cet aspect ne sera pas couvert dans le cadre de cette étude, n'ayant pas cumulé les données nécessaires à cet effet.

Pour faire suite à la recherche ayant étudié l'origine comme facteur explicatif des homicides (Ouimet, 2011), il serait intéressant de faire de même pour la cybercriminalité, crime anonyme et pour lequel il est plus difficile d'en connaître les caractéristiques puisqu'elles sont homogénéisées, que cette forme de délit est assumée comme étant identique d'un individu à l'autre et que les taux de déclaration à la police sont faibles, au contraire de l'homicide pour lequel ils sont presque de 100%.

1.4.1. Limite des différentes études

Les précédentes sections de la recension sont composées de plusieurs études comportant des limites, ce pour quoi certaines informations sont à prendre avec précaution. Les limites relevées dans ces études sont somme toute la généralisation et le faible échantillonnage. En effet, comme certains échantillons sont peu élevés (exemples : Dupont (2012) : N=10, Jackson (1994) : N=14; Holt (2009) : N=13; Turgeman-Goldschmidt (2008) : N=45, Lusthaus (2012) : N=5, Holt et Kilger (2008) :N=35, N=19, Auray et Kaminsky (2006) : N= 27, Copes et Vieraitis (2007) : N=59, Jackson (1994) N= 14), il est difficile de l'appliquer à plus grande échelle puisqu'il est possible que ça ne soit pas totalement représentatif de la population des cybercriminels (Verizon, 2012). De plus, certaines de ces études, comme celle effectuée par Franklin, Perrig, Paxson et Savage (2007), relèvent la limite portant sur la visibilité du marché. Ces auteurs ont colligé des milliers de logs sur une période de plus de sept (7) mois afin d'établir la raison d'un changement de motivation, soit de la piraterie informatique pour l'amusement à la piraterie pour le profit. Les délits étudiés dans cette recherche sont les fraudes de cartes de crédit, les vols d'identité, l'hameçonnage (le spamming), le vol de crédit en ligne et la vente des données compromises et volées. Cette limite identifie que ce qui peut être analysé est ce qui sera publicisé, accessible dans les forums, visible dans les réseaux sociaux, mais ne contient en aucun cas les messages privés envoyés entre eux ou autres éléments cachés. Ainsi, cela réduit la marge de manœuvre des scientifiques ainsi que le degré de connaissance sur le sujet. De plus, pour les études plus qualitatives, une erreur constatée est le biais d'analyse. Cela signifie que les cybercriminels, étant conscients qu'ils sont étudiés et qu'ils sont sous surveillance, vont avoir tendance à modifier leurs comportements, ce qui crée des erreurs dans les recherches (Woo, 2003). Par exemple, l'étude de Woo (2003) fut effectuée auprès de 1 385 délinquants informatiques, en provenance de 30 différents pays et qui ont participé à un sondage en ligne. Cette

étude n'était pas en lien avec le délit perpétré par le pirate informatique, mais plutôt en lien avec leurs tempéraments, leurs motivations et ce qui les amène à continuer leurs délits. Or, les réponses fournies peuvent être biaisées. Ainsi, il est difficile dans le domaine actuel d'avoir des résultats très significatifs, de par ces différentes limites.

1.5 PROBLÉMATIQUE

La cybercriminalité est un phénomène qui se fait de plus en plus connaître. En effet, les médias font davantage mention de ces délits informatiques à travers le monde. Cependant, en quoi est-ce qu'une société ou l'origine d'un délinquant peut-il produire des différences selon les caractéristiques du crime, leurs caractéristiques personnelles ainsi que motivationnelles? L'étude de Verizon (2012) a déjà établi qu'il y avait des différences entre divers continents ou régions par rapport au risque de victimisation. Cependant, il demeure intéressant de comparer ces régions entre elles et d'explorer les liens pouvant être créés avec divers paramètres tels la motivation, le degré de compétence, le type de délit, le chiffrage du préjudice, l'âge, la codélinquance, le type de victime, le nombre de victimes, le revenu, la présence d'un problème de santé mentale et le genre. Voici les limites rencontrées dans le cadre de ce mémoire et comment nous tenterons d'y pallier.

1.5.1 Limite des connaissances

La cybercriminalité n'est pas un phénomène des plus connus au niveau scientifique, ce pour quoi l'origine en tant que facteur explicatif a corsé davantage cette étude. Les études sur ce sujet ne sont pas nombreuses ou encore se situent au stade embryonnaire. En effet, il existe peu de modèles conceptuels en ce qui a trait à la cybercriminalité, et encore moins faisant référence à l'origine du

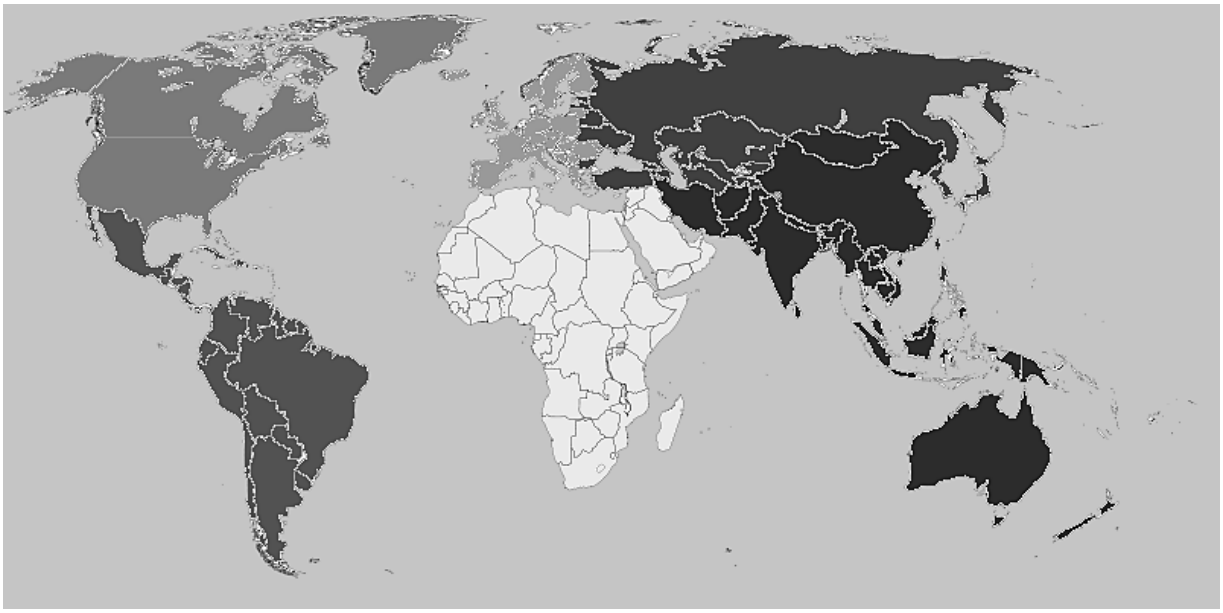
cybercriminel. De plus, peu d'études en ont fait une variable centrale et discriminante. Malgré les études ayant tenté d'accroître la compréhension quant à cette forme de criminalité peu connue et toujours grandissante, notamment les études sur la sécurité informatique ainsi que sur les conséquences financières de la cybercriminalité ayant démontré des différences au niveau mondial, telles Norton (2011), Verizon (2012), l'OECD Internet Economy Outlook (2012), L'Union Internationale des Télécommunications (2014), d'Anderson et coll. (2013), The Software Alliance (2011), aucune autre étude ne prendra l'origine en compte pour dégager les divers profils de cybercriminels. Par ailleurs, peu des études susmentionnées ont été menées dans une perspective criminologique et de nombreux liens n'ont, jusqu'à maintenant, encore jamais été créés. Malgré l'absence de modèles conceptuels, beaucoup de cadres conceptuels ont été établis à travers ces recherches qui serviront aux fins de la présente étude. Par exemple, plusieurs auteurs ont établi des typologies du cybercrime (Wall, 2003; Jordan, 2008; Holt et Bossler, 2013) ou des motivations des cyberdélinquants (Jordan et Taylor, 1998; Chiesa, Ciappi et Ducci, 2007; Simon, 2005; Jordan, 2008; Coleman et Golub, 2008), mais aucune de celles-ci ne fut mise en relation avec la provenance du cyberdélinquant, ou même en fonction d'autres variables. Ces études nous ont apporté très peu de connaissance générale quant à la piraterie à l'échelle planétaire en ce qui concerne leur type de délits, leurs types de motivation et leurs caractéristiques sociodémographiques. Elles sont limitées et réalisées dans un pays déterminé, ou n'incluent que quelques régions. D'ailleurs, il s'agit le plus souvent de pays développés, alors que l'Internet est maintenant largement répandu, même dans les sociétés en voie de développement. Il est possible d'observer qu'il existe un biais dans les études, lequel pourrait être redressé par l'étude actuelle en incluant les motivations au niveau international et de par des territoires géographiques distincts. Ainsi, grâce à la base de données qui implique des cas de délits informatiques au niveau mondial, ce

mémoire proposera différents profils de cyberdélinquants permettant d'améliorer les connaissances dans ce domaine. Ce manque au niveau des études est probablement dû à la vision homogène portée sur la cybercriminalité de par le fait que ce soit un crime produit dans un monde virtuel et qu'il ne soit pas perceptible par la population. Cela dit, la combinaison de plusieurs cadres théoriques et profils identifiés pour cette étude, et ce, en les greffant les uns aux autres et en les articulant, permettra d'obtenir des résultats généraux intéressants quant à l'origine en tant que facteur explicatif de la cyberdélinquance.

Enfin, dans la majorité des études, un problème de généralisation est à souligner. En effet, les échantillons sont très faibles, ce qui dans le cas d'une étude quantitative constitue une problématique. Le nombre de cas étudiés ne dépasse généralement pas les dizaines et est particulièrement basé sur les pirates connus par les médias, ou des pirates autodésignés dont on ne connaît pas vraiment la réelle nature délinquante. En effet, les cybercriminels les plus compétents sont les moins connus puisqu'ils réussissent à effectuer leur criminalité dans l'anonymat le plus complet, et ce, tout en esquivant les autorités. Il est ainsi impossible de refléter les résultats à l'ensemble de la population puisque la parcelle des pirates informatiques connue est celle où ils ont été arrêtés ou sont renommés dans le milieu informatique, donc non représentatif de la population au complet. Afin de contrer ce problème, l'augmentation de la taille de l'échantillonnage en créant une diversification géographique, tout en considérant des caractéristiques importantes chez les pirates lors de la sélection, permettra d'éviter la validité externe, et comme il inclut des données à l'échelle mondiale, nous tenterons de réduire le risque que la puissance statistique ainsi que la représentativité soient biaisées.

La division utilisée dans les analyses de la présente étude va comme suit: Amérique du Nord, Amérique latine, Australasie, Eurasie, Europe de l'Ouest et Afrique/ péninsule Arabique (voir Annexe 1 pour une liste des pays pour chaque catégorie). L'explication de cette division suivra plus loin. Voici une figure approximative permettant de mieux visualiser cette division :

Figure 1: Division des six (6) territoires géographiques



Il est possible de se questionner quant à la division des territoires qui se veut plutôt vaste. Cependant, celle-ci permettra d'établir une base théorique quant à l'impact de l'origine sur les comportements cybercriminels et ce, d'autant plus que la recherche se veut exploratoire, suite à quoi des tests plus poussés pourront être effectués.

1.5.2 Démarches et objectifs

L'objectif général de ce mémoire est de décrire le profil des cybercriminels et cyberdélinquants recensés dans les médias internationaux. Plus précisément, l'objectif est de

pouvoir établir de nouvelles connaissances quant aux différences de ces profils en fonction du pays d'origine du cyberdélinquant. Ainsi, la base de données est créée en divisant les cas de cybercriminels retrouvés sur divers moteurs de recherches et en fonction de leur origine. L'origine se voudra donc le facteur explicatif des différentes caractéristiques du crime informatique. Nous créerons des associations avec nos diverses variables indépendantes, soit le type de motivation, le degré de compétence, le type de délit, l'âge, la codélinquance, le type de victime, la provenance des victimes, le revenu obtenu, la sentence obtenue, le nombre de pseudonymes utilisés, l'appartenance à un groupe, la présence d'un problème de santé mentale et le sexe.

Non seulement le mémoire vise à créer des associations, mais il aspire aussi à vérifier si ces profils varient selon le lieu d'origine du cyberdélinquant. On retrouvera dans la section opérationnalisation des variables la justification du choix de ces variables. L'étude sera principalement exploratoire et tentera de créer une connaissance plus diversifiée de ce phénomène à l'échelle mondiale tout en sélectionnant les divers cadres conceptuels les plus appropriés.

1.5.3 Différents profils ciblés

Afin d'y parvenir et compte tenu du manque de données et d'informations explicatives quant à la criminalité informatique en fonction de l'origine géographique du cyberdélinquant, il est intéressant de soumettre différents profils et lignes directrices qui guideront l'analyse de cette étude et qui sont créés à l'aide des différents territoires géographiques ciblés. Ces profils sont centrés sur la théorie des opportunités criminelles et des activités routinières (Cohen et

Felson, 1979; Cusson, 2002) et ce, en fonction de la motivation selon l'origine, incluant les opportunités légitimes et l'accès à Internet, qui ne sont pas les mêmes d'un endroit à l'autre.

Avant tout, voici quelques explicatifs quant à la théorie des opportunités criminelles et des activités routinières. D'abord, ces théories tournent autour de la présence de trois acteurs : les délinquants, les victimes potentielles, et le gardien. Cohen et Felson (1979) identifient que les habitudes de vies sont à la source des opportunités, tout comme le sont les occasions favorables exposées au moment où le délinquant veut passer à l'action (Cusson, 2002). Nous pouvons appliquer cette théorie dans le cadre de la cybercriminalité, puisque l'augmentation de la propension des technologies, notamment l'accès à Internet, aura une incidence sur les occasions criminelles. Par exemple, des individus qui n'ont pas l'habitude de protéger leur ordinateur ou de renouveler l'antivirus lorsqu'il est expiré offrent une meilleure opportunité aux cyberdélinquants d'infiltrer leur système ou de frauder leurs données personnelles. Ces mauvaises habitudes de vie auront donc pour effet de favoriser ce type de criminalité. Quant aux occasions criminelles, si au moment de passer à l'acte le délinquant n'est pas dissuadé par un gardien, s'il y a absence de témoins, s'il est placé devant l'occasion idéale pour perpétrer un délit sans qu'aucun facteur dissuasif ne soit réuni, il passera conséquemment à l'acte. De plus, les opportunités d'emploi, les inégalités financières, l'accessibilité aux ressources technologiques ainsi que l'accès à Internet, différents d'un territoire géographique à l'autre, auront une incidence sur les opportunités exposées au cyberdélinquant. Suite à une balance décisionnelle, si la perpétration du délit entraîne plus d'avantages que de désavantages, il s'y adonnera. Or, la prévention situationnelle est importante afin de contrer cette problématique, mais encore bien peu présente dans le cas de la cybercriminalité.

En nous fiant aux études dans lesquelles des comparatifs de crimes au plan mondial ont déjà été effectués, nous avons formulé quelques profils typiques des pirates informatiques selon leur provenance. D'abord, on s'attend à voir une proportion plus importante de pirates être motivés par l'appât du gain dans les pays en voie de développement ou en transition économique, où les opportunités économiques sont réduites de par la présence d'inégalités au niveau des revenus, que dans les pays développés, où les opportunités financières sont élargies. Les besoins des habitants varieront entre ces divers pays ou continents, tant au niveau des besoins matériels et de la facilité d'acquisition d'outils technologiques que des besoins financiers. Ainsi, des pirates informatiques se trouvant dans une situation économique plus précaire utiliseraient-ils la voie de la criminalité afin de subvenir à leurs besoins financiers? Les unités géographiques qui sont davantage ciblées ici sont l'Afrique/péninsule Arabique, l'Amérique latine ainsi que l'Eurasie.

Pour les pirates présentant une motivation idéologique ou politique, il serait possible de les trouver relativement plus fréquemment dans les régions où il y a présence de conflits armés autant civils que transfrontaliers, de conflits sociopolitiques, ou même dans les pays où l'accès à Internet est simplifié. D'abord, l'Europe de l'Ouest et l'Amérique du Nord ont un accès simplifié à Internet. En effet, si nous nous référons aux réseaux Internet, l'Europe de l'Ouest, l'Eurasie et l'Amérique du Nord sont les mieux équipées (Akamai, 2013). Cet accès leur donne une plus grande facilité, de meilleures occasions quant à la commission de crimes informatiques plus élaborés, comme l'infiltration et ce, dans le but de faire valoir une opinion et un point de vue, donc de se faire entendre par le gouvernement et/ou les groupes politiques,

notamment par des mouvements sociaux auxquels Anonymous et d'autres groupes apportent leur soutien. Internet n'est pas facilement accessible pour tous les pays du monde et ils ne peuvent pas tous en faire un usage rapide. Ainsi, un pirate désirant s'infiltrer dans des ordinateurs, à l'aide d'un mode opératoire plutôt complexe, n'aura pas la même facilité dans un pays où les réseaux ne s'étendent pas convenablement jusqu'à sa circonscription, comparé à un pays où Internet est la voie principale pour toutes les communications et qui est à sa vitesse maximale. Il s'agit en fait d'opportunisme, puisque les conditions propices à la commission du délit auront été réunies, notamment les circonstances et l'environnement favorisant cet accès à Internet (Cohen et Felons, 1979). De plus, comme certains conflits armés persistent, il serait possible que des délinquants informatiques en provenance de ces pays désirent faire valoir leur opinion. Par exemple: les conflits armés, les tensions politiques et problèmes humanitaires de la Russie contre l'Ukraine, ayant donné lieu à des cyberattaques répertoriées (Ross, 2014; L'OBS Actualié, 2014) ainsi que la cyberguerre d'Israël contre l'Iran (Benillouche, 2010; Untersinger, 2012; OBS, 2010). Il est possible que d'autres conflits ne soient actuellement pas cités, mais ces derniers, somme toute importants, font office d'exemples dans le but de soutenir le fait que des conflits subsistent, d'où certaines personnes pourraient être plus propices à vouloir montrer leur désaccord par l'intermédiaire de la cybercriminalité.

Afin d'avoir un guide au niveau de la vitesse d'Internet en fonction de l'origine, caractéristique qui varie d'un territoire à l'autre et qui peut avoir un effet sur les opportunités criminelles, l'étude d'Akamai (2013) rapporte les différentes moyennes de la vitesse d'Internet au niveau international. Voici dans le I un récapitulatif des positions occupées par divers pays pertinents dans le cadre de l'étude actuelle :

Tableau I

Rang occupé par les pays au niveau de la vitesse Internet

Territoire géographique	**Pays**	**Position**
Amérique du Nord	Canada	15e
	États Unis	8e
Europe de l'Ouest	Pays-Bas	4e
	Suisse	5e
	Belgique	9e
	France	34e
Eurasie	Russie	20e
	Hongrie	33e
	Roumanie	21e
	Slovénie	31e
Australasie	Australie	43e
	Corée du Sud	1er
	Japon	2e
	Inde	123e
Afrique/péninsule Arabique	Israël	16e
	Émirats Arabes Unis	51e
	Afrique du Sud	95e
Amérique latine	Mexique	57e
	Brésil	84e
	Argentine	80e

Toutefois, la différence entre les rangs plutôt rapprochés n'est pas des plus significatives. Or, ces résultats sont à prendre avec attention et considération. Cette classification pourra de ce fait même aider à obtenir des pistes quant à l'accessibilité et la vitesse des réseaux informatiques par les cybercriminels selon leur provenance, et ainsi le type de délit qu'ils pourraient accomplir.

CHAPITRE 2 : MÉTHODOLOGIE

Ce chapitre a pour but d'éclairer le lecteur quant aux sources de la base de données, la formation de celle-ci, par rapport à l'opérationnalisation des variables, tout comme la stratégie analytique utilisée, soit les tests statistiques qui seront effectués dans le cadre de cette recherche.

2.1 SOURCE DES DONNÉES

Afin de bien situer le lecteur, il est d'abord important de décrire et de donner des informations quant à la source des données soit la division des territoires géographiques, la procédure de la création de la base de données ainsi que le choix des participants et finalement, les défis et limites rencontrés lors des procédures de création de cette base de données.

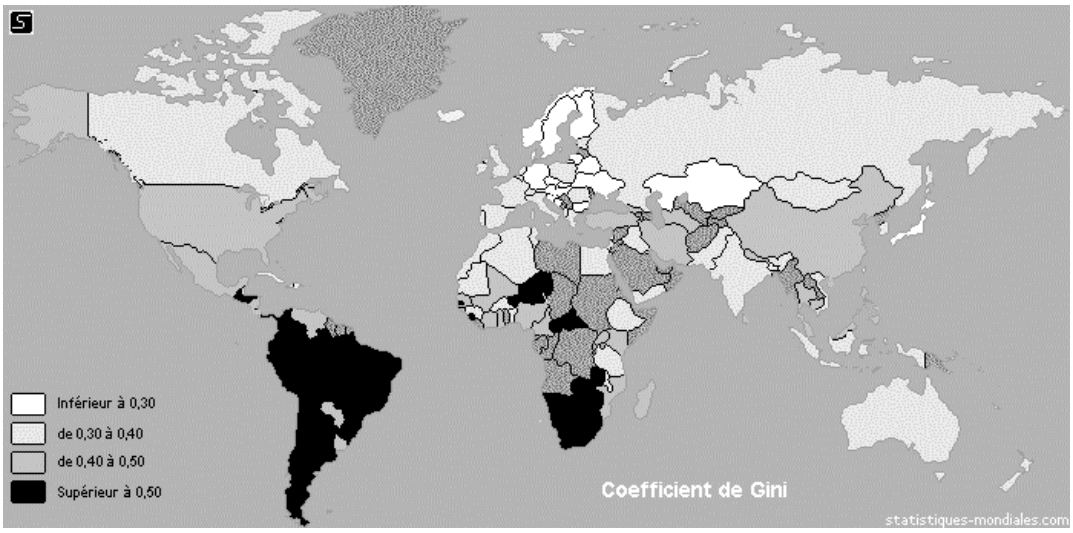
2.1.1 Division des territoires géographiques

D'emblée, il a été étudié dans le domaine de la criminologie que des différences notables existent dans les formes de délinquances selon la provenance de l'individu, la société dans laquelle il a été élevé, et ce, sous la pression de divers facteurs, par exemple l'étude sur les homicides de Mucchielli (2002) et de Ouimet (2011), la théorie de l'Anomie de Durkheim (Merton, 1938), l'étude sur la pauvreté et les homicides influençant le taux d'incarcération de Ouimet (2012), l'étude du lien entre la religion et les homicides de Leroux (2013), l'étude entre l'économie et la criminalité de Soullez (2014) et autres. Ainsi, afin de pouvoir explorer les divergences en ce qui a trait à la cybercriminalité, la division des territoires a généralement été effectuée par continent, où des ressemblances étaient relevées quant aux caractéristiques économiques et démographiques. Malgré que des différences peuvent subsister à l'intérieur

d'un même pays, une évaluation globale des différentes situations politiques, économiques et sociales nous a permis de conclure que cette division serait la moins restreignante pour l'étude actuelle et que dans le cadre d'une recherche exploratoire, c'était une délimitation des plus intéressantes. Nous sommes d'avis que cette division sépare bien les pays les plus distincts et aura pour effet d'apporter un nouvel angle de recherche au sujet de la cybercriminalité. Cette division est basée sur les territoires d'origine des délinquants, de leur provenance géographique et non les territoires de provenance de leurs victimes ou du lieu où sont les systèmes qu'ils attaquent. À rappeler que la division des six territoires est la suivante: Amérique du Nord, Amérique latine, Australasie, Eurasie, Europe de l'Ouest et Afrique/ péninsule Arabique.

Par ailleurs, si nous nous fions au coefficient de Gini, il est possible de remarquer que la division de ces territoires correspond globalement à la division des inégalités et égalités financières régnant entre les différentes régions. Ce coefficient permet de mesurer les inégalités des revenus dans un même pays. Lorsque le coefficient se rapproche de 0, c'est que les revenus sont équitablement distribués. Dans le sens inverse, lorsqu'il se rapproche de 1, c'est qu'il y a une inégalité totale subsistant dans le pays (Statistiques mondiales, 2014). Voici une carte, repérée sur le site de Statistiques mondiales, permettant d'avoir une vue d'ensemble des iniquités financières.

Figure 2: Coefficient de Gini par pays



2.1.2 Procédures de création de la base de données, choix des participants

La base de données utilisée aux fins de la présente étude a entièrement été conçue puisqu'il n'existait aucun échantillon adéquat en lien avec le sujet de recherche actuel et qu'il est pertinent d'explorer les différences des cybercriminels selon leur origine. La récolte des données fut effectuée entre le mois de septembre 2013 et le mois de février 2014. L'échantillonnage a été mené sur une courte période, compte tenu des restrictions temporelles. Les variables sont de nature qualitative, mais les données sont quantitatives. Effectivement, il est question de motivation, de type de criminalité, bref, de variables nominales pour lesquelles il n'est pas possible d'effectuer de tests statistiques. Afin de parvenir à une analyse quantitative, une opérationnalisation des variables fut effectuée. L'objectif était de créer un échantillon constitué de pirates informatiques ou de cybercriminels provenant de partout dans le monde, ayant été arrêtés ou tout simplement ceux étant connus pour leurs délits informatiques. Il n'y avait aucun critère spécifique quant à l'année de la commission du délit puisque la base de données aurait largement été restreinte, tout comme pour

l'âge du délinquant. L'année du délit fut malgré tout notée dans la base de données en tant que référence advenant un besoin futur, mais n'est en aucun cas déterminante dans la présente étude.

Pour chacun des territoires énumérés dans la section précédente, l'objectif était de trouver quinze (15) cas de cybercriminels, totalisant un échantillon de N=90. La technique employée afin de recueillir ce nombre de cyberdélinquants fut une recherche d'abord aléatoire des cas médiatisés dans des moteurs de recherche telle Google, Google news et Hackers News. Google News, ou Google Actualités, est en fait un moteur de recherche incluant 50 000 sources médiatiques, distribuées en 70 différentes langues et éditions régionales (Google News, 2014). Les articles proposés par ce moteur de recherche sont tous filtrés et classés par thèmes et en ordre de pertinence et de notoriété, s'étendant à l'échelle mondiale et sur pratiquement tous les sujets possibles. Quant à Hackers News (http://thehackernews.com), c'est aussi un moteur de recherche recueillant et compilant les meilleurs articles et ressources au niveau mondial. Cette base de recherche est cependant spécialisée en matière de sécurité informatique. Les mots clés utilisés afin de trouver ces cyberdélinquants étaient les suivants : « hackers », pirates informatiques, cybercriminels, cyberdélinquants, cybercriminel et cybercrime. De plus, afin de compléter la base de données et de trouver des « hackers » en fonction des territoires manquants, l'ajout au mot clé d'un territoire était effectué, par exemple : « hackers » + Amérique du Nord, pirates + Brésil, « hackers » + Europe, « hackers » + origine, cybercriminalité + pays, etc. Nous avons procédé ainsi pour chacun des territoires, ce qui nous a permis de cumuler quinze (15) cas par région identifiée. Les mots clés choisis sont relatifs au domaine à l'étude, soit la cybercriminalité. Ils devaient être plus généraux compte tenu de l'aspect exploratoire de notre recherche et que nous tentions de recueillir tous les cas possibles. Nous n'avons pas choisi des mots clés trop sélectifs puisque s'ils avaient été trop précis, il aurait été difficile de compléter la banque de

données et d'en faire les analyses. D'établir des mots clés précis tels : fraudeurs, infiltration informatique, etc., aurait généré un biais de sélection considérable puisque le type de délit récolté aurait été établi en fonction de ces recherches concises et non aléatoirement et que conséquemment, nos analyses n'auraient plus été représentatives. Nous n'aurions pu identifier que tel délit est plus représentatif de tels territoires puisque nous aurions provoqué l'ajout de cette variable à notre base de données.

Un seul critère important devait être d'emblée satisfait lors de la sélection des cyberdélinquants afin de monter une base de données nous permettant d'obtenir des résultats significatifs: la provenance géographique. Lorsqu'un cyberdélinquant répondant à ce critère de base était identifié, soit en réponse à une arrestation ou à une forte notoriété, il était enregistré dans la base de données, et ce, toujours en fonction de sa provenance géographique. Ensuite, les recherches portant sur son délit étaient approfondies, en lisant plusieurs autres articles à son sujet. Ainsi, les données ont été colligées principalement pour faire suite à la lecture des articles diffusés par divers médias. La sélection était en premier lieu aléatoire, dans le sens où les cas furent enregistrés au fil des trouvailles, sans jamais être exclus de la base de données. Toutefois, la recherche fut ensuite plus sélective. Un choix de cas fut effectué en second lieu, en fonction des critères de sélection et des variables à l'étude. Lorsqu'une déficience au niveau des informations était remarquée, soit par exemple s'il n'y avait ni la motivation du délinquant, ni le type du délit, ni le type de victime, nous jugions inadéquat de retenir ce cas de cybercriminalité. Environ 70 cas ont ainsi été exclus. Comme l'étude actuelle vise à faire des associations entre divers paramètres ainsi que l'origine du cyberdélinquant, soit la motivation, le type de délit, l'âge, le sexe, la codélinquance, le type de victime, la provenance des victimes, le revenu obtenu, l'appartenance à un groupe, la présence d'un problème de santé mentale,

la sentence obtenue et l'occupation du délinquant au moment du délit, ces cas trop incomplets ne répondaient pas à l'objectif.

Bref, les critères d'échantillonnage sont bien simples : détenir l'origine du cybercriminel ainsi que son âge. Ensuite, les autres paramètres établis furent remplis en fonction des informations mentionnées dans les divers articles.

Il est important de rappeler le biais de sélection à l'effet que les données de l'étude actuelle ont été colligées par des moteurs de recherche Internet, fournissant des articles de cas médiatisés. Effectivement, les médias préfèrent certaines histoires de par leur trame narrative, leur côté atypique. Ceci peut amener une surreprésentation de certains crimes ou du type de motivation. Or, la base de données est constituée de cybercriminels dont le crime ou la notoriété était si important qu'il aura attiré l'attention des médias. Bien que ces informations en provenance des médias puissent être faussées et parfois manquer d'authenticité, cette base de données est une source crédible dans le cadre de la présente étude. En effet, les informations recueillies des médias font l'objet de vérifications auprès de plusieurs sources appliquant des critères rigoureux de journalisme afin de contrôler leur fiabilité. De plus, la source Internet où les informations furent retenues devait être fiable, soit en provenance d'un média établi et connu pour la crédibilité de ses informations. Par exemple, une publication dans un forum n'était pas assez fiable pour en enregistrer les informations. Mentionnons que peu de contradictions n'étaient relevées d'un article à l'autre, sinon aucune, ce qui facilitait la création de la base de données et diminuait les chances d'obtenir des informations biaisées.

2.1.3 Défis et limites des procédures de création de la base de données

Il fut, à certains moments, plus ardu de créer cette base de données. Certains défis furent surmontés au long du processus. Il est important de soulever quelques limites ayant été rencontrées lors de la création de cette base de données.

2.1.3.1 Création des territoires

Premièrement, nous avons utilisé des unités géographiques scindées généralement en fonction des divisions continentales. Il fut jugé que cette division était adéquate dans le cadre de l'étude actuelle à caractère exploratoire. Cependant, cette division peut engendrer des résultats biaisés dans le sens où les critères culturels, religieux, sociaux et économiques peuvent largement différer, et ce, malgré la proximité des régions.

Par exemple, au niveau économique, soit le revenu par habitant par année, un grand clivage est présent entre le Cambodge (950$ US) et le Japon (46 140$ US), tout comme entre Haïti (810$ US) et les Bahamas (20 600$ US) et ce, malgré la proximité de ces pays et que ceux-ci soient inclus dans le même territoire géographique pour l'étude actuelle (Banque Mondiale, 2014). De plus, le Brésil est exclu de notre étude, se traduisant par une limite compte tenu de l'importance de la cybercriminalité dans ce pays, mais surtout du manque d'informations complètes de cybercriminels en provenance de ce territoire géographique. Effectivement, le Brésil est un foyer important de pirates informatiques (mi2g Intelligence

Unit, 2002). Nous pouvons traduire cette absence d'information soit parce que les services de police ont peu d'intérêt à les retracer et les arrêter ou soit parce qu'il y a un manque de médiatisation de tels cas dans ce pays. Or, il n'y a pas de pirates informatiques en provenance de ce pays dans la base de données actuelle.

Quant à l'aspect religieux, prenons pour exemple que certains pays sont eux-mêmes composés de diverses religions, telle l'Arabie, où l'islam et l'hindouisme sont présents ainsi que le Tchad où le judaïsme, quoique marginal, et l'islam sont les religions présentes. En Afrique, trois pays voisins ont différentes religions, soit la Somalie étant islamique, l'Éthiopie d'inspiration chrétienne et le Kenya catholique protestant (Arte, 2011).

En ce qui a trait au niveau politique et social, des conflits armés perdurent dans divers pays du monde, comme ceux en Europe de l'Est, tout comme certains en Asie, en Afrique et dans la péninsule Arabique. Certains conflits politiques persistent aussi en Europe de l'Ouest. Ainsi, il est possible de voir que la division des territoires géographiques englobe certains conflits ayant des impacts différents au niveau social et politique, et ce, dans une même unité géographique. Les motivations de cyberdélinquants, tout comme leurs moyens pour parvenir à la commission du délit, peuvent donc différer d'un pays à l'autre, mais seront combinées en un seul territoire géographique, ce qui consiste en une limite importante pour l'étude actuelle.

Tout compte fait, comme le but de ce mémoire est d'explorer à l'échelle mondiale et d'établir des bases de recherche quant à l'origine comme facteur explicatif, nous avons opté pour cette division. Une division territoriale en fonction des pays ainsi que de leurs

caractéristiques propres aurait pu être réalisée, mais aurait été de trop grande envergure pour un mémoire de maîtrise puisqu'un échantillon de taille minimale aurait dû être identifié pour chaque pays. De plus, nous voulions éviter d'avoir un échantillon trop faible pour prévenir le biais de généralisation, ce pour quoi nous avons opté pour une division plus globale. Il serait ainsi intéressant éventuellement de jeter un œil aux différences entre les divers paramètres ciblés, mais ce, en fonction des pays. Cette piste serait matière à exploration future.

2.1.3.2 Échantillonnage

Ensuite, l'échantillon de la base de données n'est pas des plus élevés, soit N=90. Selon le peu de temps disponible pour réaliser la présente étude ainsi que les ressources limitées, il n'était pas évident de cumuler suffisamment de données permettant d'augmenter la taille de l'échantillon. Devant cette contrainte temporelle, nous avons tout de même fait un travail de qualité dans les démarches de collecte de nos données. Également, de par cet échantillon plus faible, il se peut qu'aucun résultat significatif ne soit obtenu et qu'aucune relation ne soit considérée quand dans les faits, il en existe une. Cependant, afin de contrer ce problème, la considération des caractéristiques importantes chez les pirates lors de la sélection a permis d'éviter la généralisation trop rapide, et comme cet échantillon s'étend à l'échelle mondiale par plusieurs catégories de pays, le risque que la puissance statistique ainsi que la représentativité soient biaisées est réduit. Malgré tout, en comparant cet échantillon aux échantillons des diverses études précédentes sur le sujet (exemples : Dupont (2012) : N=10, Jackson (1994) : N=14; Holt (2009) : N=13); Turgeman-Goldschmidt (2008) : N=45, Lusthaus (2012) : N=5, Holt et Kilger (2008) :N=35, N=19, Auray et Kaminsky (2006) : N= 27, Copes et Vieraitis (2007) : N=59, Jackson

(1994) N= 14), il est possible d'affirmer qu'il est plus élevé dans le cadre d'une recherche quantitative. Il faudra tout de même être attentif à ne pas tomber dans un processus de généralisation.

2.1.3.3. *Biais de sélection*

Dans une étude pour laquelle le temps alloué à la recherche est restreint, il est difficile d'accumuler des centaines de cas de cybercriminalité, ce pour quoi la sélection est de 15 cas de cybercriminels par régions identifiées (référence à la limite précédente). D'ailleurs, il existe plus d'articles de cybercriminels en provenance de certaines régions et moins pour d'autres, ce qui créait une certaine marge au niveau de l'accumulation des cas. Effectivement, au fil des recherches, certaines données étaient encore manquantes, par exemple pour la région de l'Amérique latine, mais un surplus de données était observé au niveau de la région de l'Amérique du Nord, et ce, malgré l'ajout de certains mots clés plus spécifiques à chacun des territoires. La majorité des noms en surplus trouvés aléatoirement furent initialement conservés, malgré le déséquilibre créé entre les données cumulées pour chaque territoire (voir tableau II). Cependant, une sélection parmi les cas plus nombreux pour une région où la cyberdélinquance est plus répandue était de mise. Or, le biais de sélection de la recherche consiste dans le fait que pour la sélection des quinze (15) cybercriminels, ceux pour lesquels il y avait le plus d'information furent conservés au détriment des cas les moins enrichis. Ceci peut subsister en une faiblesse puisqu'un cybercriminel pour qui il existe davantage d'information est en fait un cas ayant été davantage médiatisé pour plusieurs raisons, entre autres l'ampleur de son délit ou tout simplement sa notoriété. Cette sélection peut ainsi s'avérer discriminatoire et réduire l'échantillon à des cas plus lourds ou connus. Une tentative de contrer la généralisation dans la présente étude fut alors effectuée, soit en augmentant le nombre de pirates

informatiques analysés (N= 90). Le Tableau II indique le nombre de cas trouvés initialement pour chaque territoire.

Tableau II
Nombre de cas recensés par territoire géographique

Amérique du Nord	38
Amérique latine	16
Australasie	35
Europe de l'Ouest	22
Eurasie	28
Afrique/péninsule Arabique	29

2.2 OPÉRATIONNALISATION DES VARIABLES

La section de l'opérationnalisation des variables permettra d'identifier les variables utilisées aux fins de la présente étude ainsi que la catégorisation de ces dernières, tout comme l'opérationnalisation de la variable discriminante à l'étude. De plus, elle permettra d'avoir un aperçu de notre échantillon.

2.2.1 Variables utilisées

Les variables ont été choisies afin de mieux connaître le phénomène de la cybercriminalité. Le degré de compétence du délinquant sera-t-il tributaire de l'accès qu'il a à Internet, ou tout simplement à un ordinateur? Est-ce que les types de délits, de motivations et de victimes, varieront d'un territoire à l'autre, en fonction de l'accès aux ressources et selon les inégalités financières? De plus, il est intéressant d'étudier si le phénomène se produit majoritairement seul ou en groupe. Certains territoires géographiques peuvent revendiquer davantage la liberté d'expression et des groupes de pirates en sont le résultat (Anonymous, Lulzsec, etc.). Ce sont

en partie ces variables qui fourniront certaines réponses et qui permettront d'établir les différences par rapport à l'origine du cyberdélinquant, et ce, au plan international. Voici une exploration plus en détail de ces différentes variables.

D'abord, une des variables utilisées est le type de délit commis par le cyberdélinquant. Au niveau de cette variable, il sera pertinent d'explorer si les inégalités financières et l'accès à Internet sont un enjeu dans le type de délit perpétré. Cette variable est nominale et fut déterminée en fonction de la catégorisation de Holt et Bossler (2014). La catégorisation de cette étude est une des plus récentes, globalisant les diverses typologies formulées par maints auteurs, ce pour quoi elle fut sélectionnée dans le cadre de la recherche actuelle. Il s'agit donc des types de délits suivants: infiltration=1, fraude=2, cyberpornographie/obscénité=3, cyberviolence=4 ou autre=0. Cependant, les attaques informatiques ont été rajoutées à la catégorisation de Holt et Bossler, à cause de leur fréquence. Ainsi, les attaques sont opérationnalisées comme suit : Attaques informatiques =5. Pour cette variable, l'échantillon est de N=90. La distribution sera explorée plus loin, mais mentionnons tout de même d'emblée que dans la base de données, aucun délit n'est de nature cyberponographique/obscène ni de nature cyberviolente. La cueillette fut aléatoire, et aucun délit de cette nature ne fut récolté, possiblement puisque ce sont des délits moraux de plus grande gravité pour lesquels les médias n'ont pas suffisamment d'information ou pour lesquels les mots clés ne correspondaient pas de par leur généralité.

Ensuite, la motivation du cyberdélinquant à perpétrer ce délit sera prise en compte. La motivation se définit, selon le Larousse (2014), comme étant les «raisons, intérêts, éléments qui poussent quelqu'un dans son action ; fait pour quelqu'un d'être motivé à agir». Il est

intéressant d'inclure cette variable dans l'étude afin de vérifier si l'intérêt des cyberdélinquants varie d'un territoire à l'autre. Cette variable a été créée avec, en tant que références, les catégorisations de Jordan et Taylor (1998), Rogers (2006) ainsi que Chiesa, Ciappi et Ducci (2007). Les éléments les plus pertinents et fréquents furent retenus et combinés, formant la catégorisation suivante: 0= inconnue, profit=1, curiosité=2, idéologie=3, ennui=4, ou espionnage étatique=5. Par profit, il est entendu tout crime commis dans le but d'obtenir un gain financier, donc par l'appât du gain. Pour ce qui est de la curiosité, il est question des délits perpétrés par les délinquants désireux d'en apprendre davantage sur le monde informatique. Ensuite, le caractère idéologique du délit est au niveau des contestations quant aux intérêts politiques ou nationaux. L'ennui est évidemment la motivation où un délinquant désire s'occuper et opte pour la complexité des délits informatiques. L'espionnage étatique est un délit d'ordre politique, où des crimes informatiques seront commis dans le but d'obtenir des informations sur les gouvernements étrangers ou autres entreprises, par des vols de données stratégiques (Colin, 2012). Cependant, dans la base de données actuelle, aucun délit n'est motivé par l'espionnage étatique, possiblement de par son caractère secret et privé. Finalement, la catégorie «inconnue» englobe les cas où la motivation n'était pas mentionnée. Toutefois, les catégories susmentionnées sont les plus communes et incluent la majorité des cas. La variable du type de motivation du cyberdélinquant est de nature nominale. Elle était recueillie dans les divers articles médiatiques. Dans cette base de données, la prise en compte des motivations multiples n'est pas possible puisque les cas retenus n'avaient qu'une motivation prédominante. L'échantillon correspondant à cette variable est de N=90.

Vient ensuite la variable ordinale du degré de compétence, typologie tirée de l'étude de Verizon (2012). Tout d'abord, la compétence du délinquant peut être évaluée sur une échelle de quatre (4) items, soit inconnue =0, très faible =1, faible=2, modérée=3 et élevée=4 (N=90). Ces différents niveaux sont tous jugés sur les mêmes notions, soit le niveau d'habiletés du délinquant, la touche de personnalisation qu'il apportera dans ses démarches ainsi que les ressources l'entourant. Premièrement, le très faible degré de compétence est en fait celui où tout individu se situe, où aucune habileté technique, sociale, intuitive ou de connaissance n'est acquise. Deuxièmement, le faible degré de compétence comprend les cyberdélinquants ayant des techniques de base ou possédant quelques ressources afin de les guider. Par exemple, dans le domaine informatique et à ce degré de compétence, ce seraient des «outils automatiques et des scripts» qui sont utilisés par les délinquants, sans même qu'ils aient ajouté une légère touche personnelle (Verizon, 2012). Troisièmement, le degré de compétence modéré inclut de meilleures habiletés à tous les différents stades. En effet, les délinquants sauront comment utiliser les différentes ressources à leur disposition, étant d'ailleurs plus nombreuses, et pourront par conséquent apporter quelques modifications aux virus ou autres, compte tenu de leurs acquis et connaissances plus développés. Finalement, le degré de compétence élevé tient compte des individus ayant des habiletés informatiques très avancées et qui par conséquent, seront en mesure de procéder à leurs délits grâce à leurs propres programmes, applications ou créations informatiques personnalisées (scripts).

En ce qui a trait à la variable nominale du type de victime visé par le cybercriminel, elle est déterminée comme suit: Gouvernements/écoles=1, entreprises/banques/commerces=2, médias=3, partis politiques/associations politiques=4 ou individus=5. La taille de l'échantillon

est de N=90. Afin de faciliter la lecture du mémoire, nous utiliserons les termes simplifiés de gouvernements, d'entreprises, de médias, de partis politiques et d'individus.

L'origine des victimes fut déterminée en fonction de la même catégorisation que l'origine du cybercriminel soit : Amérique du Nord=0, Amérique latine=1, Australasie=2, Eurasie=3, Europe de l'Ouest=4 et péninsule Arabique/Afrique=5. La différence avec l'opérationnalisation de l'origine du cybercriminel résulte dans l'ajout de l'option mondiale =6, puisque parfois les victimes des cybercriminels s'étendaient à l'échelle internationale, et inconnue =7. L'échantillon pour cette variable nominale est de N=90.

L'occupation du délinquant est aussi une variable nominale intéressante aux fins de la présente étude. Effectivement, il est intéressant de savoir si le pirate avait un statut professionnel=1, éducationnel=2, s'il n'occupait aucun de ces statuts=3 ou s'il était inconnu=0. L'échantillon de cette variable s'élève à N=90. Il sera aussi intéressant dans la section des résultats de prendre en compte, sur un plan qualitatif, quels sont les types d'emploi occupés par ces cybercriminels, tout comme le cycle de formation atteint par les cybercriminels aux études. Comme peu d'informations ont été trouvées en ce qui a trait à l'emploi, ou le cycle d'études atteint, ils ne seront cités qu'à titre informatif.

En ce qui concerne les variables démographiques, l'âge fut enregistré en tant que variable continue. Cette variable ne sera pas catégorisée puisque l'idée est d'avoir une moyenne approximative des cyberdélinquants, en fonction de leur pays d'origine. Le nombre

de cas pour cette variable est de N=90. En ce qui a trait au genre, la variable fut évidemment dichotomisée, soit 0 pour les hommes et 1 pour les femmes, l'échantillon étant de N=90.

Dans le cas échéant, il serait convenable de se pencher sur la codélinquance. Effectivement, est-ce majoritairement des crimes commis seuls, avec un autre individu ou en groupe? Cette variable a été codée comme suit : présence d'un codélinquant Non=0 et Oui=1. L'échantillon pour cette variable dichotomique est de N=90. De plus, le nombre de codélinquants fut aussi enregistré dans la base de données afin d'établir une moyenne, ce qui consiste en une variable continue (N=90).

En ce qui concerne l'appartenance à un groupe, la variable fut codée ainsi : aucun =0, Anonymous = 1, LulzSec = 2, autre = 3. C'est une variable nominale avec un échantillon de N=90. Nous ne jugions pas pertinent de créer la catégorie inconnue pour la variable de l'appartenance à un groupe puisque cette information est très médiatisée. Nous concluons donc que si le cyberdélinquant faisait partie d'un groupe, il aurait été mentionné dans l'article autrement, il n'était affilié à aucun groupe.

De plus sont inclus les délinquants présentant des ou un trouble de santé mentale, ou non, tel le syndrome d'Asperger, dépendance aux substances, dépendance affective ou dépression. Elle fut opérationnalisée comme Non=0 et Oui=1. L'échantillon pour cette variable dichotomique est de N=90. Nous n'avons pas créé une troisième catégorie «inconnue» parce que les articles médiatisés vont révéler la présence d'un trouble de santé mentale si tel est le cas, mais en revanche, ils ne spécifieront pas si l'information est

manquante ou s'il y a absence de trouble de santé mentale. Or, le «non» inclut les pirates informatiques ne présentant aucun trouble ou ceux dont nous n'avons pas l'information. Or, les tests statistiques à cet effet risquent d'être moins précis et devront être manipulés avec soin.

Également, le montant obtenu suite au délit sera analysé. Si le cybercriminel avait obtenu un revenu de sa criminalité, il était codé Oui= 1. S'il n'y avait aucun revenu ou qu'il n'en y avait mention dans aucun article, il était noté Non=0. L'échantillon de cette variable dichotomique est de N= 90. Il est important de soulever ici que la manière dont les auteurs des divers articles ont procédé au calcul des revenus n'est pas connue. Il est possible que certains auteurs aient scindé le profit cumulé par le crime et le revenu, et que certains auteurs aient considéré le profit à part du revenu. Ainsi, ces variations du calcul du revenu peuvent engendrer un biais significatif des résultats dans le sens où il n'y a pas de base de calcul du revenu uniforme à chacun.

Finalement, il sera intéressant de se pencher sur la sentence obtenue en fonction du pays d'origine du cyberdélinquant (N=90). Cette variable est nominale. Les codifications vont comme suit : 0= aucune, 1= amende et travaux compensatoires, 2= peine privative de liberté et probation, 3= amende et peine privative de liberté, et finalement, 4= inconnue. Nous avons procédé à ces regroupements puisqu'il était rare dans tous les cas recensés qu'il n'y avait qu'une seule sentence octroyée au cyberdélinquant. Nous avons donc optimisé les chances d'obtenir des résultats en évitant de sélectionner une des peines obtenues pour chacun des cas en créant ces divisions.

2.2.2 Variable discriminante

Aux fins de cette étude, une seule variable discriminante sera utilisée, soit l'origine du cybercriminel. Elle subsiste en la variable prédominante et centrale de l'étude puisque c'est le facteur qui, selon nous, déterminera le profil des cyberdélinquants. Il s'agit d'une variable nominale et l'échantillon de celle-ci est de N=90. La catégorisation se fait ainsi : Amérique du Nord=0, Amérique latine=1, Australasie=2, Eurasie=3, Europe de l'Ouest=4 et péninsule Arabique/Afrique=5.

2.3 STRATÉGIE ANALYTIQUE

Maintenant que nous avons eu une vue d'ensemble sur les différentes variables à l'étude, voici les stratégies et les tests statistiques qui seront utilisés. Il y aura d'abord un récapitulatif des tests statistiques univariés et ensuite, la description des stratégies déployées afin de procéder aux tests statistiques bivariés.

2.3.1 Tests statistiques univariés

L'objectif de notre étude est de comparer les différentes variables en fonction de l'origine. Il demeure toutefois intéressant d'avoir une vue d'ensemble sur la cybercriminalité, celle-ci s'appliquant au niveau mondial. De ce fait, des analyses univariées, plus précisément des tests de fréquence, ont été effectuées sur l'ensemble des données recueillies internationalement, pouvant par conséquent donner une idée générale des caractéristiques de ce type de criminalité. Ces analyses ont aussi comme objectif de décrire l'échantillon de notre recherche. Une fois ces tests effectués, nous procéderons aux tests statistiques plus poussés.

2.3.2 Tests statistiques bivariés

En premier lieu, il sera intéressant de vérifier les liens entre les diverses variables à l'étude, sans tenir compte de la variable discriminante. Or, des tests de tableaux croisés, ou tableaux de contingence seront effectués. C'est ce type de test qui a été sélectionné compte tenu de la nature des variables, soit deux variables qualitatives nominales. De plus, ce choix de test offrira une continuité avec les tests statistiques de la section suivante. L'objectif de ces analyses est de discerner si certaines variables présentent une relation étroite, et ce, afin de déterminer s'il existe des risques de relations fallacieuses ou tout simplement d'établir s'il existe une relation intéressante entre ces variables. Une fois les variables croisées, nous procéderons au croisement des sous-catégories afin de vérifier s'il existe des relations plus précises entre ces dernières. D'ailleurs, l'indice de force sera identifié et est catégorisé comme suit : 0 = absence de relation; 0,05-0,10 = très faible relation; 0,10-0,20 = faible relation ; 0,20-0,40 = relation modérée; 0,40-0,80 = forte relation et finalement 0,80-1,00 = relation qui semble fallacieuse. En second lieu, des tests de moyennes seront effectués, plus précisément à l'aide du test de moyenne non paramétrique de Kruskal-Wallis puisque les postulats des tests de moyennes ne pouvaient être respectés, notamment que chacune des catégories doit avoir un échantillon de plus de trente cas ($N \geq 30$).

Ensuite, des tableaux de contingence seront effectués entre la variable discriminante, soit le pays d'origine du cyberdélinquant, ainsi que les autres variables utilisées. Ce type de test permettra d'établir si les délinquants informatiques en provenance des diverses régions commettent des délits semblables ou s'ils possèdent des caractéristiques criminelles et

personnelles différentes. Évidemment, ce test ne permet en aucun cas d'établir une relation de cause à effet, mais permet d'établir s'il y a une association existante entre ces deux variables. De plus, ces tableaux permettront d'avoir une vue d'ensemble sur la distribution des différentes variables en fonction de chacune des régions. Cette distribution sera identifiée en pourcentage dans les tableaux. Toutefois, comme le postulat exigeant un minimum de cinq observations dans chaque case ($N \geq 5$) ne sera pas respecté pour certaines variables, nous nous en tiendrons uniquement à la présentation des tableaux ainsi qu'à la description de la distribution. Pour les différences plus importantes qui y seront observées, nous nous référerons à de seconds tests, soit les tableaux de contingence avec un ajustement Bonferroni. Or, ces tests permettront de ne pas violer le postulat de base des chi-deux, celui où l'échantillon pour chacune des variables croisées doit être supérieur à cinq (5).

Voici le processus établi pour effectuer ces seconds tests statistiques bivariés, soit avec l'ajustement Bonferroni. Comme il y a six (6) différentes régions, il serait risqué de les comparer toutes au même moment puisqu'il pourrait résulter des erreurs statistiques, soit plus précisément l'erreur de type 1, où certaines différences ou corrélations entre les variables pourraient être assumées lorsque dans les faits il n'en existe aucune (Fox, 1999). Effectivement, de nombreuses comparaisons entre des variables peuvent amener divers problèmes au niveau de l'interprétation et de l'analyse, soit obtenir des différences indûment significatives. Afin d'éviter le tout, un «fractionnement du risque d'erreur» est nécessaire (Jouan-Flahault, Casset-Semanez et Minini, 2004). Dans le cadre de l'étude actuelle, il y aura un total de quinze (15) tableaux croisés, ce qui augmente les risques d'avoir des différences significatives biaisées d'au moins 40%. Par conséquent, un ajustement Bonferroni a été

nécessaire, et ce, compte tenu du nombre de tests statistiques élevé à effectuer. Cet ajustement consiste en une division des seuils de signification initiaux par le nombre de tests effectués, soit dans le cas échéant 15 tests ($p \leq 0,05$; $p \leq 0,01$; $p \leq 0,001$). Ce processus a résulté en de faibles seuils de signification, soit $p \leq 0,003$ plutôt que $p \leq 0,05$, $p \leq 0,0007$ plutôt que $p \leq 0,01$ ainsi que $p \leq 0,00007$ plutôt que $p \leq 0,001$. Ainsi, cette procédure réduira les chances d'obtenir des résultats erronés. Cependant, ces seuils de signification réduits auront pour effet de diminuer les chances d'obtenir des résultats significatifs, ce qui complique quelque peu l'étude. Les tableaux croisés seront réalisés en combinant deux unités géographiques à la fois, soit par exemple : Amérique du Nord avec Amérique latine, Amérique du Nord avec Australasie, Amérique du Nord avec Europe de l'Ouest, etc. Subséquemment, advenant l'obtention de résultats significatifs dans les analyses statistiques bivariées, il y aura moins de doutes quant à la fiabilité de ceux-ci. De plus, les variables seront dichotomisées afin de pouvoir procéder à ces tests de tableau croisés avec l'ajustement Bonferroni, soit par exemple l'infiltration oui= 1, non=0, attaques informatiques oui=1, non=0 et fraude oui=1, non =0, etc.

CHAPITRE 3 : RÉSULTATS DES ANALYSES UNIVARIÉES

Maintenant que l'explication de la procédure des tests a été réalisée, ce chapitre consiste à fournir les résultats obtenus par les tests univariés. En premier lieu, des analyses de fréquence ont été réalisées en fonction des variables démographiques : l'âge et le sexe. Il appert que l'âge moyen de l'échantillon disponible mondialement (N=89) est d'environ 25 ans. Cette variable est distribuée de façon normale. L'étendue de l'âge varie de 12 ans à 46 ans. Quant à la mesure des quartiles, elle indique que 25% des cybercriminels sont âgés de 20 ans et moins, 50% de 24 ans et moins et 75% de 28 ans et moins. Cette large étendue nous permet d'observer que ce type de criminalité n'est pas spécifique à un âge, mais s'étend bien de la jeune adolescence à l'âge adulte, contrairement à ce que la majorité des études révèlent. Malgré le fait que dans la majorité des cas les cyberdélinquants ne soient pas âgés de plus de 28 ans, il n'en demeure pas moins que les différentes études recensées identifient l'âge moyen des cybercriminels à environ 18 ans et que notre étude relève uniquement 25% de cas âgés de moins de 20 ans.

En ce qui concerne l'âge autodéclaré d'entrée en piraterie, l'analyse a été effectuée sur un échantillon plus restreint, soit de 19 cas confondant toutes les régions. Ainsi, l'âge moyen d'entrée en piraterie est d'environ 16 ans, l'âge minimum étant de 6 ans et le maximum de 32 ans. L'échantillon de cette analyse est limité, ce qui peut expliquer la différence avec les études où l'âge d'entrée en piraterie est évalué de 8 à 11 ans.

Quant à la variable associée au genre des individus commettant la cybercriminalité, les résultats révèlent une présence majoritairement masculine. Sur l'échantillon total, le ratio est

de 89 hommes (98,9%) pour 1 femme (1,1%). Il est intéressant de faire ici le parallèle avec les précédentes études, qui avaient aussi relevé la masculinité de ce type de criminalité. Ce résultat vient par conséquent confirmer la surreprésentation du genre masculin en ce qui concerne la cybercriminalité. D'ailleurs, la seule femme incluse dans l'étude actuelle, âgée de 27 ans, est originaire du Mexique et a commis un délit de nature frauduleuse, avec comme victimes des individus. Cette dernière a un degré de compétence très faible, ayant utilisé les informations de cartes de crédit volées, et ce, dans le but de faire des achats personnels.

Dans ce même ordre d'idées, la distribution du degré de compétence des cyberdélinquants va comme suit : 33,3% présentent un très faible degré de compétence, 30% un faible degré de compétence, 11,1% un degré de compétence modéré et 23,3% un degré de compétence élevé. Notre échantillon est bien différent de celui de l'étude de Verizon (2011), où les délinquants présentaient majoritairement des degrés de compétence modérés (39%) et faibles (30%). Ceci peut s'expliquer par la nature des délits sélectionnés dans le cadre de leur étude, étant principalement en lien avec des intrusions informatiques. Or, notre échantillon considère également les délits de fraudes et d'attaques informatiques, ce qui produit des résultats différents.

Ensuite, l'analyse du nombre de codélinquants lors de l'acte délictuel révèle que sur l'échantillon total, 66,7% des cyberdélinquants ont agi de pair avec en moyenne environ un autre individu (N=90). Cette variable s'étend de 0 à 6 codélinquants, la moyenne étant de 1,39 et le mode de 1. Ce résultat est distinct de celui des études recensées, où il fut relevé que dans

70% des cas les pirates ont agi seuls. Quant à l'appartenance à un groupe de cyberdélinquants, 72,2% (N=90) des cyberdélinquants n'appartiennent à aucun groupe de pirates. Ceux dans un groupe appartiennent dans 12,2% des cas à Anonymous, 8,9% à LulzSec et 6,7% des cas à un autre groupe. Toutefois, le fait de ne pas appartenir à un groupe de délinquants n'exclut pas la possibilité d'avoir commis le délit accompagné d'un autre individu. Le Tableau III présence ces résultats ainsi que ceux qui suivront.

Tableau III
Description de l'échantillon

	Moyenne (x)	Mode (m)	Écart-type (S)	(N)	Min	Max
Âge	25,30	27	6,74	89	12	46
Âge d'entrée en piraterie	16,00	16	7,196	19	6	32
Nombre de codélinquants	1,39	1	1,619	90	0	6
Nombre de surnoms	1,43	1	1,529	90	0	8
Sexe (N=90)	**N**		**%**			
Femme	1		1,1			
Homme	89		98,9			
Type de délit (N=90)	**N**		**%**			
Infiltration	44		48,9			
Attaque	25		27,8			
Fraude	19		21,1			
Autres	2		2,2			
Cyberpornographie	0		0			
Cyberviolence	0		0			
Motivation (N=90)	**N**		**%**			
Profit	46		51,1			
Idéologie	24		25,6			
Inconnue	8		13,3			
Curiosité	6		4,4			
Ennui	6		5,6			
Espionnage étatique	0		0			
Occupation (N=90)	**N**		**%**			
Inconnue	47		52,2			
Profession	28		31,1			
Éducation	11		12,2			
Aucune	4		4,4			
Revenu (N=90)	**N**		**%**			
Oui	22		24,4			
Non	68		75,6			
Groupe (N=90)	**N**		**%**			
Anonymous	11		12,2			
Lulzsec	8		8,9			
Autre	6		6,7			
Aucun	65		72,2			
Type de Victime (N=90)	**N**		**%**			
Gouvernement	32		35,6			
Entreprise	38		44,2			
Individu	20		22,2			
Partis politiques	0		0			
Médias	0		0			
Provenance des victimes (N=90)	**N**		**%**			
Amérique du Nord	37		41,1			

Amérique latine	7	7,8
Australasie	12	13,3
Europe de l'Ouest	3	3,3
Eurasie	1	1,1
Afr./péninsule Arabique	6	6,7
Monde	17	18,9
Inconnu	7	7,8
Codélinquance (N=90)	**N**	**%**
Oui	60	66,7
Non	30	33,3
Degré de compétence (N=90)	**N**	**%**
Très faible	30	33,3
Faible	27	30
Modéré	10	11,1
Élevé	21	23,3
Inconnu	2	2,2
Santé mentale (N=90)	**N**	**%**
Oui	9	10
Non	81	90
Sentence obtenue (N=90)	**N**	**%**
Aucune	12	13,3
Amende / travaux compensatoires	3	3,3
Peine privative de liberté/probation	24	26,7
Amende et peine privative de liberté	23	25,6
Inconnue	28	31,1

Toujours à l'échelle internationale, voici quelques statistiques descriptives effectuées au niveau des autres variables. D'abord, sur le plan du type de délit (N=90), c'est l'infiltration qui est le plus perpétrée, soit à 48,9%, suivit des attaques informatiques, à 27,8%. Vient ensuite la fraude, à 21,1% et finalement, les délits autres à 2,2%. La motivation de ces délinquants est d'emblée le profit obtenu suite à leur crime (51,1%), suivie du caractère idéologique motivant le crime à 26,7% (N=90). Les résultats en lien avec notre échantillon ne coïncident pas avec ceux représentés dans la recension des écrits, lesquels reflétaient que c'est d'emblée la curiosité qui primait, suivie de l'expérience qu'apporte cette criminalité (Holt et Schell, 2010). Effectivement, dans notre cas, la proportion des cyberdélinquants motivés par la curiosité ne représente que 4,4% de l'échantillon. Cette différence peut être en lien avec la médiatisation de nos cas, ce qui évoque des délits plus importants donc des cyberdélinquants qui présenteront conséquemment une motivation plus sérieuse.

Les cibles les plus visées sont les entreprises commerciales et les banques, soit à 44,2%, comparées à 35,6% pour les gouvernements, universités ou services de santé. C'est dans 22,2% des cas que les individus furent personnellement victimes des attaques de ces cybercriminels (N=90). Ceci rappelle les résultats obtenus dans l'étude de Hollinger (1991), où les entreprises de grande envergure seront davantage ciblées que des individus. Quant à la provenance de ces victimes, 41,1% sont originaires de l'Amérique du Nord, 18,9% de partout dans le monde, 13,3% de l'Australasie, 7,8% de l'Amérique latine et 6,7% d'Afrique/péninsule Arabique (N=90).

Subséquemment, sur l'échantillon total, soit N=90, 75,6% des cybercriminels n'ont pas obtenu de revenu suite à la perpétration de leur délit. Pour ce qui est du 24,4% des criminels ayant obtenu un revenu, donc sur les 22 cas où le revenu était connu, celui-ci s'élève en moyenne à 229 530$ (min= 3 730$, max= 1 million $).

Il est également intéressant d'avoir un aperçu des conséquences économiques en obtenant le chiffrage du préjudice (N=61). La moyenne des préjudices causés est d'environ 33 millions de dollars. Il y a tout de même une étendue importante entre le préjudice le plus bas, étant de 2 055$ et le plus élevé, 866 millions de dollars. Le mode de cette variable, soit le montant du préjudice le plus fréquent, est de 10 millions de dollars. Le préjudice de 866 millions de dollars est en lien avec la création d'un programme, créé par un cyberdélinquant originaire de Russie du nom de Dmitry Fetodov, âgé de 35 ans. Le programme a été utilisé par divers groupes criminels organisés pour siphonner l'argent de plusieurs banques, ce pour quoi ce montant est aussi élevé.

En ce qui a trait à l'occupation de ces criminels, elle est majoritairement inconnue, soit à 52,2%. Par contre, pour ceux où il fut possible de distinguer l'occupation (N=43), 31,1% des cas avaient une occupation professionnelle, 12,2% des cas une occupation éducationnelle, et 4,4% des cas n'en avait aucune, bénéficiaient notamment du service d'assurance emploi. Bien que cet échantillon soit incomplet, cela vient infirmer les stéréotypes des cybercriminels n'ayant aucun emploi, jeunes étudiants n'ayant un intérêt que pour la technologie.

Les cyberdélinquants ayant un trouble de santé mentale diagnostiqué représentent 10% de l'échantillon total de N=89. Certains d'entre eux (N=9) avaient le syndrome d'Asperger, souffraient de dépression, d'anxiété généralisée, comme d'autres de troubles bipolaires. Il est possible d'observer que quatre (4) de ces neuf (9) délinquants ont le syndrome d'Asperger. Malgré le fait que cet échantillon soit plutôt restreint, le syndrome d'Asperger est présent dans le profil de certains cybercriminels, mais ne peut être généralisé à la population entière puisqu'ils devaient tout simplement représenter des cas intéressants à médiatiser. Ce faible pourcentage peut aussi être expliqué par l'absence d'un diagnostic de ce syndrome ou de ces troubles ou par le fait que la santé mentale n'est pas prédictrice de ce type de criminalité. C'est une piste qui demeure intéressante à étudier davantage dans de futures études.

En ce qui a trait à la sentence obtenue, il est possible d'observer que celles incluant la peine privative de liberté et la probation (26,7%) ainsi que l'amende et la peine privative de liberté (25,6%) sont les plus octroyées. La surreprésentation de ce type de sentence est

probablement liée au fait que ce sont des cas tirés d'articles médiatiques, des cas plus intéressants et de gravité plus importante, donc pour lesquels la peine sera plus sérieuse.

En définitive, le nombre de pseudonymes des cybercriminels est évalué en moyenne à 1,43 surnom. Le minimum est de 0 surnom, et le maximum est de 8 surnoms empruntés par ces délinquants informatiques. Un large écart persiste entre ceux-ci, pouvant être expliqué par le fait que certains cyberdélinquants étaient plus impliqués dans la cybercriminalité, dans les communautés informatiques ainsi que dans divers forums de cyberdélinquants, de là la nécessité d'avoir plusieurs surnoms.

Ce bref survol des statistiques descriptives englobant les cybercriminels en provenance de divers territoires géographiques nous permet d'avoir une idée générale de ce type de criminalité. Effectivement, l'infiltration est le type de délit le plus fréquent. Un lien peut être créé avec la motivation idéologique importante où les délinquants s'attaquent beaucoup aux gouvernements, universités et services de santé. Ensuite, la fraude est le troisième type de délit le plus important, les entreprises commerciales et les banques étant les cibles les plus importantes des cybercriminels, le tout motivé par le profit obtenu de ces crimes, étant somme toute la motivation la plus populaire au monde, et ce, toujours en fonction de l'échantillon actuel.

Cette description de l'échantillon est intéressante et les analyses fournissent une vue d'ensemble de l'échantillon à l'étude, ce qui est peu proposé dans la littérature étudiant la cybercriminalité. Effectivement, notre échantillon est plus complet et prend en considération

plusieurs variables afin de voir plus tard s'il existe des relations entre elles, plutôt que de se centrer uniquement sur une variable, par exemple la motivation, comme certaines études le font. Ces tests n'établissent cependant aucune comparaison des différentes variables à l'étude et nous voulons savoir s'il existe de réelles relations entre les variables susmentionnées permettant de dégager un profil plus typique du cyberdélinquant. Les tests de tableaux croisés sont donc nécessaires dans l'approfondissement des analyses et seront présentés dans le chapitre suivant, suite à quoi il sera intéressant de croiser ces variables avec celle de l'origine, objectif premier de notre étude.

CHAPITRE 4 : RÉSULTATS DES ANALYSES BIVARIÉES

4.1 ANALYSES DE TABLEAUX DE CONTINGENCE ENTRE LES VARIABLES À L'ÉTUDE

Des tests de tableaux de contingence ont d'abord été effectués entre les variables à l'étude afin de savoir s'il existe des relations entre ces dernières. Un premier tableau de contingence servira à croiser les variables globales, et nous procéderons aux tableaux croisés des variables dichotomisées afin de comparer les sous-variables et ainsi ne pas violer le postulat de plus de cinq observations par cellule.

4.1.1 Type de délit et type de victime

Nous avons d'abord effectué un tableau croisé entre la variable du type de délit et du type de victime (Tableau IV). Nous pouvons observer de par la distribution de ces variables que les cyberdélinquants commettant des délits d'infiltrations ciblent davantage les entreprises, ceux perpétrant des délits de fraudes visent plus les individus et ceux commettant des attaques informatiques auront dans leur mire les entreprises.

Tableau IV
Tableau croisé du type de délit et du type de victime

	Gouvernement(%)	Entreprises(%)	Individu(%)
Autre	-	50	50
Infiltration	61,4	29,5	9,1
Fraude	10,5	42,1	47,4
Attaque	12	64	24

*V de Cramer= 0,410***; *p≤0,05; **p≤0,01; ***p≤0,001*

Il existe une forte relation entre les délits d'infiltrations et les victimes gouvernementales (Phi= 0,527; p≤0,001), où les délinquants commettant ce type de délit (61,4%) viseront davantage les gouvernements que les cyberdélinquants ne procédant pas ainsi

(10,9%) (N=30). Afin de bien situer les lecteurs, les pourcentages utilisés sont utiles pour l'interprétation du sens de la relation identifiée, soit si elle est négative ou positive.

Toujours selon le type de délit d'infiltration, les délinquants utilisant ce mode opératoire seront moins nombreux à cibler les entreprises (29,5%) que ceux utilisant un type de délit différent (54,3%) (N=30). La force de cette relation négative est modérée (Phi= -0,251; $p \leq 0,05$). Il en est de même pour les victimes individuelles, moins ciblées par les cyberdélinquants commettant des délits d'infiltration (9,1%) que ceux n'en commettant pas (34,8%) (N=30). La force de cette relation négative est identifiée comme modérée selon le Phi de -0,309 ($p \leq 0,01$).

Nous avons également croisé les délits d'attaques informatiques avec les victimes corporatives. Il existe une relation modérément significative entre ces variables (Phi= 0,273; $p \leq 0,05$). Les délinquants perpétrant des attaques informatiques cibleront davantage les entreprises (64%) que ceux n'utilisant pas ce mode opératoire (33,8%) (N=30).

Pour ce qui est du délit de fraude, nous pouvons observer qu'il existe une relation significative modérée avec les victimes individuelles (Phi= 0,313; $p \leq 0,01$). Effectivement, les cybercriminels employant la criminalité frauduleuse auront davantage dans leur mire les victimes individuelles (47,4%) que ceux adoptant un type de criminalité différant (15,5%) (N=30).

Il existe également une relation statistiquement significative entre les délits de fraudes et les victimes gouvernementales. Les cyberdélinquants employant la fraude comme délit sont moins à même de cibler les gouvernements (10,5%) que ceux n'employant pas ce moyen (42,4%). La force de cette relation négative est évaluée comme étant modérée, comme en témoigne le Phi de -0,270 ($p \leq 0,05$) (N=30).

4.1.2 Type de délit et type de motivation

Ensuite, nous voulions voir s'il existe des relations entre le type de délit employé par le cyberdélinquant ainsi que leur motivation à commettre ce délit. Rapidement, nous pouvons voir qu'il y a un pourcentage élevé entre la fraude et le profit, l'infiltration et l'idéologie ainsi que les attaques informatiques et le profit (Tableau V). Or, afin de vérifier s'il existe des relations significatives, nous avons procédé aux tests de tableaux croisés dichotomisés pour chacune des variables.

Tableau V
Tableau croisé du type de délit et du type de motivation

	Inconnue(%)	Profit(%)	Curiosité(%)	Idéologie(%)	Ennui(%)
Autre	-	50	-	50	-
Infiltration	13,6	27,3	4,5	45,5	9,1
Fraude	-	100	-	-	-
Attaque	24	56	8	8	4

*V de Cramer= 0,375***;*p≤0,05; **p≤0,01; ***p≤0,001*

D'abord, il existe une forte relation statistiquement significative entre les délinquants perpétrant de la fraude et ceux étant motivés par le profit (Phi= 0,515; $p \leq 0,001$). Effectivement, les cyberdélinquants commettants de la fraude sont davantage motivés par le

profit (100%) que ceux n'en commettant pas (38%) (N=30). En revanche, les délinquants commettant ce type de délit sont moins motivés (0%) par le caractère idéologique que ceux procédant autrement (32,4%). Cette relation négative est évaluée comme étant de force modérée selon le Phi (-0,303; p≤ 0,01) (N=30).

Ensuite, il existe une relation significative entre les délits intrusifs et la motivation idéologique. Cette relation est évaluée comme étant forte (Phi = 0,446; p≤ 0,001). Les délinquants utilisant l'infiltration comme type de délit sont davantage motivés par le caractère idéologique de leurs actions (45,5%) que ceux utilisant un autre mode opératoire (6,5%). Il existe également une forte relation négative entre ce type de délit et la motivation du profit (Phi= -0,466; p≤ 0,001). Effectivement, les délinquants empruntant ce mode opératoire sont moins motivés par le profit (27,3%) que ceux ne l'employant pas (73,9%) (N=30).

4.1.3 Type de délit et degré de compétence

Voici maintenant le tableau des résultats en lien avec le croisement des variables du type de délit et du degré de compétence (Tableau VI). Il est pertinent de savoir s'il existe une relation entre le choix du délit ainsi que les techniques et habiletés que présente le cyberdélinquant.

Tableau VI
Tableau croisé du type de délit et du degré de compétence

	Inconnu(%)	Très faible(%)	Faible(%)	Modéré(%)	Élevé(%)
Autre	-	-	-	-	100
Infiltration	-	38,6	31,8	15,9	13,6
Fraude	10,5	52,6	31,6	-	5,3
Attaque	-	12	28	12	48

*V de Cramer= 0,355***; *p≤0,05; **p≤0,01; ***p≤0,001*

Les résultats qui semblent marquants sont au niveau du type de délit de fraude et du degré de compétence très faible, ainsi que les délits autres avec le degré de compétence élevé. Nous pouvons aussi voir un résultat statistique élevé pour les attaques informatiques et le degré de compétence élevé.

D'abord, aucune relation statistiquement significative n'existe entre le type de délit de fraude et le très faible degré de compétence. Ensuite, il existe une relation statistiquement significative entre les délits autres et le degré de compétence élevé, de force modérée (Phi = 0,282; $p \leq 0,05$). Les délinquants commettant les délits autres sont plus nombreux à avoir un degré de compétence élevé (100%) que ceux commettant des délits d'infiltration, de fraude et d'attaques informatiques (20,5%) (N=30).

En ce qui a trait au croisement entre la variable des cyberdélinquants commettant des attaques informatiques ainsi que le degré de compétence élevé, il appert qu'il existe une relation significative modérée (Phi= 0,325; $p \leq 0,01$). Effectivement, les cybercriminels ayant comme mode opératoire les attaques informatiques ont un degré de compétence plus élevé (44,4%) que ceux ne procédant pas ainsi (13,8%) (N=30).

4.1.4 Type de motivation et type de crime

Également, nous trouvions intéressant de croiser le type de motivation avec le type de victime (Tableau VII). Effectivement, comme nous avons croisé le type de délit avec la motivation ainsi qu'avec le type de victime, il est pertinent de croiser le type de motivation

avec le type de victime afin de voir s'il n'y aurait pas une analyse pertinente à apporter entre toutes ces variables.

Tableau VII
Tableau croisé du type de motivation et du type de victime

	Gouvernement(%)	Entreprises(%)	Individu(%)
Inconnue	41,7	41,7	16,7
Profit	8,7	54,3	37
Curiosité	75	25	-
Idéologie	73,9	21,7	4,3
Ennui	60	40	-

*V de Cramer= 0,445***; *p≤0,05; **p≤0,01; ***p≤0,001*

De ce tableau, il est possible de relever une différence qui semble importante entre les statistiques de la motivation idéologique et des victimes gouvernementales. Existe-t-il aussi une relation entre le délit motivé par le profit et les victimes corporatives? Qu'en est-il de la motivation de curiosité et des victimes gouvernementales?

Dans les faits, il existe une forte relation statistiquement significative entre les délinquants présentant une motivation idéologique et ciblant les gouvernements (Phi=0,469; p≤ 0,001). Ils sont plus nombreux à les viser (73,9%) que ceux présentant un autre type de motivation (22,4%) (N=30). Toutefois, ils sont moins nombreux à cibler les entreprises (21,7%) que ceux ayant une autre motivation (49,3%), relation négative qui s'avère être de force modérée (Phi= -0,243; p≤0,05) (N=30). Il en est de même pour les victimes individuelles, étant moins ciblées par les délinquants motivés par l'idéologie (4,3%) que ceux présentant un autre type de motivation (28,4%) (N=30). Cette relation négative est de force modérée (Phi= - 0,252; p≤ 0,05).

D'autre part, une relation statistiquement significative existe entre la variable des cyberdélinquants motivés par le profit et ceux qui ont les entreprises dans leur mire. Cette relation est de force modérée (Phi = 0,251; p≤ 0,05). Les délinquants motivés par le profit visent davantage les entreprises (54,3%) que ceux présentant une autre motivation (29,5%) (N=30). De plus, il appert que les délinquants motivés par le profit seront moins nombreux (8,7%) que les délinquants présentant un autre type de motivation (63,6%) à viser les gouvernements, relation négative qui est évaluée comme étant de force élevée comme en témoigne le Phi de -0,574 (p≤ 0,001) (N=30). Toujours selon les cyberdélinquants motivés par le profit, ils sont plus nombreux à cibler les victimes individuelles (37%) que ceux présentant une autre motivation (6,8%) (N=30). La force de cette relation est estimée comme modérée (Phi= 0,362; p≤ 0,001).

4.1.5 Type de motivation et degré de compétence

Nous avons ensuite effectué des tests de tableaux de contingence entre les variables du type de motivation et du degré de compétence du cybercriminel. Le tableau révèle différentes statistiques obtenues en faisant le premier croisement entre ces variables. Nous avons ensuite procédé au croisement des variables dichotomiques afin de nous assurer de la fiabilité des relations identifiées, les résultats étant présentés dans le tableau VIII. Uniquement deux relations statistiquement significatives sont observées.

Tableau VIII
Tableau croisé du type de motivation et du degré de compétence

	Inconnu(%)	Très faible(%)	Faible(%)	Modéré(%)	Élevé(%)
Inconnue	-	16,7	50	8,3	25

Profit	4,3	37	30,4	2,2	26,1
Curiosité	-	25	25	25	25
Idéologie	-	39,1	26,1	13	21,7
Ennui	-	20	0	80	0

*V de Cramer= 0,306**; *p≤0,05; **p≤0,01; ***p≤0,001*

Il existe d'abord une relation statistiquement significative entre la motivation de l'ennui ainsi que le degré de compétence de niveau modéré. Cette relation est évaluée comme étant forte (Phi = 0,472; p≤ 0,001). Effectivement, les délinquants motivés par l'ennui sont plus nombreux à avoir un degré de compétence modéré (80%) que ceux présentant une autre motivation (7,1%) (N=30).

Ensuite, il subsiste une relation significative entre la motivation du profit ainsi que le degré de compétence de niveau modéré. Les cyberdélinquants motivés par le profit qui présentent un degré de compétence modéré sont moins nombreux (2,2%) que les délinquants présentant une autre motivation (20,5%) (N=30). Cette relation négative est de force modérée comme en témoigne le Phi de -0,291 (p≤ 0,05).

4.1.6 Type de motivation et revenu obtenu

Nous avons également jugé pertinent de croiser la variable du revenu obtenu de la criminalité avec le type de motivation et le type de délit. Nous retrouvons les résultats de la distribution dans le Tableau IX. À première vue, il semble exister une relation entre la variable du profit et du revenu obtenu. Les tests de tableaux de contingence entre les deux variables dichotomiques nous révèleront s'il en existe réellement une.

Tableau IX
Tableau croisé de la motivation et du revenu obtenu

	Non (%)	Oui (%)
Inconnue	83,3	16,7
Profit	65,2	34,8
Curiosité	100	-
Idéologie	82,6	17,4
Ennui	100	-

*V de Cramer= 0,271 ; *p≤ 0,05; **p≤ 0,01; ***p≤ 0,001*

Effectivement, il existe une relation statistiquement significative. Les cyberdélinquants motivés par le profit sont plus nombreux (35,6%) à avoir obtenu un revenu que ceux présentant une autre motivation (13,6%) (N=30). Cette relation est de force modérée, comme en témoigne le Phi de 0,254 (p≤ 0,05).

4.1.7 Type de délit et revenu obtenu

Quant aux relations statistiquement significatives identifiées entre le type de délit effectué ainsi que le revenu obtenu, elles sont observées pour les types de délits suivants : infiltration et fraude. Les délinquants perpétrant des délits intrusifs sont moins nombreux à obtenir un revenu (11,4%), que ceux n'utilisant pas l'infiltration (37%) (N=30). Cette relation négative est catégorisée comme force modérée (Phi= -0,298; p≤ 0,01). Également, les délinquants commettants de la fraude sont plus nombreux à obtenir un revenu de leur délit (41,1%) que ceux utilisant un autre mode opératoire (19,7%) (N=30). Quant à la force de la relation, elle est modérée (Phi= 0,213; p≤ 0,05). Voici ici-bas le Tableau X de la distribution de ces variables.

Tableau X
Tableau croisé du type de délit et du revenu obtenu

	Non (%)	Oui (%)
Autre	-	100
Infiltration	88,6	11,4
Fraude	57.9	42,1
Attaques	72	28

*V de Cramer= 0,389** ; *p≤ 0,05; **p≤ 0,01; ***p≤ 0,001*

4.1.8 Type de motivation et appartenance à un groupe

Il existe des relations statistiquement significatives entre la variable du profit et celle de l'appartenance à un groupe. De la distribution de ces variables, il semble que les délinquants motivés par l'idéologie soient plus nombreux à appartenir au groupe Anonymous, ceux motivés par l'ennui au groupe LulzSec et ceux motivés par le profit à aucun groupe. Les résultats de la distribution sont présentés dans le tableau XI.

Tableau XI
Tableau croisé du type de motivation et de l'appartenance à un groupe

	Autre	Anonymous	LulzSec	Aucun
Inconnue	8,3	8,3	-	83,3
Profit	6,5	-	-	93,5
Curiosité	-	-	25	75
Idéologie	8,7	43,5	21,7	26,1
Ennui	0	0	40	60

*V de cramer= 0,306**; *p≤ 0,05; **p≤0,01; ***p≤0,001*

D'abord, ceux motivés par le profit sont moins nombreux (0%) à appartenir au groupe Anonymous que ceux présentant une autre motivation (25%) (N=30). Cette relation négative présente une force modérée, comme en témoigne le Phi de -0,382 (p≤ 0,001). Il existe également une relation négative de force modérée entre ce type de motivation et l'appartenance au groupe LulzSec (Phi = -0,319; p≤ 0,01). Les délinquants motivés par le

profit sont moins nombreux à appartenir à ce groupe (0%) que ceux présentant une autre motivation (18,2%) (N=30). D'autre part, les délinquants motivés par le gain financier ont plus de chance de n'appartenir à aucun groupe (93,5%), comparé à ceux présentant une autre motivation (47,7%) (N=30). Cette relation est évaluée comme présentant une force élevée, comme en assure le Phi de 0,505 ($p \leq 0,001$).

Il est également intéressant de constater qu'il existe une forte relation statistiquement significative au niveau de la motivation idéologique et du groupe Anonymous (Phi = 0,559; $p \leq 0,001$). Les délinquants présentant une motivation idéologique sont plus nombreux à faire partie du groupe Anonymous (43,3%) que ceux n'étant pas motivés par l'idéologie (1,5%) (N=30).

Toujours selon cette motivation, il existe une relation significative avec la variable de l'appartenance au groupe LulzSec. Cette relation est moins forte que la précédente et est identifiée comme modérée (Phi= 0,265; $p \leq 0,05$). Les délinquants motivés par l'idéologie appartiennent davantage au groupe LulzSec (21,7%) que ceux ne l'étant pas (4,5%) (N=30). En revanche, les délinquants motivés par l'idéologie sont moins nombreux à n'appartenir à aucun groupe de cyberdélinquants (21,7%) que ceux présentant une autre motivation (88,1%) (N=30). Cette relation statistiquement significative présente une force élevée (Phi = -0,638; $p \leq 0,001$). Ces résultats nous permettent de croire que lorsqu'un délinquant présente une motivation idéologique, les chances qu'il appartienne à un groupe sont plus élevées.

4.1.9 Type de motivation et codélinquance

D'abord, les cyberdélinquants présentant une motivation inconnue sont moins nombreux à avoir des codélinquants (25%) que ceux ayant une autre motivation (74%) (N=30). La force de la relation négative statistiquement significative entre ces deux variables est modérée, comme le souligne le Phi de -0,380 ($p \leq 0,001$).

De plus, il existe une relation statiquement significative modérée entre les délinquants motivés par le profit ainsi que la codélinquance (Phi = 0,251; $p \leq 0,05$). Les délinquants motivés par le profit sont plus nombreux (78,3%) à agir avec d'autres délinquants que ceux présentant une autre motivation (54,5%) (N=30). Le tableau XII suivant présente la distribution des résultats.

Tableau XII
Tableau croisé du type de motivation et de la codélinquance

	Non (%)	Oui (%)
Inconnue	75	25
Profit	21,7	78,3
Curiosité	25	75
Idéologie	39,1	60.9
Ennui	20	80

V de Cramer=0,381; *p≤0,05; **p≤0,01; ***p≤0,001*

4.1.10 Degré de compétence et revenu obtenu

En ce qui a trait au croisement entre le degré de compétence et le revenu obtenu (Tableau XIII), une relation statistiquement significative nous paraît intéressante. Effectivement, les délinquants présentant un degré de compétence élevé sont plus nombreux à obtenir un revenu de leur criminalité (45%) versus ceux présentant un autre niveau de compétence (18,6%)

(N=30). La force de cette relation est évaluée comme modérée (Phi= 0,256; p≤ 0,05). Le tableau suivant présente les résultats statistiques obtenus lors du croisement des variables du degré de compétence et du revenu obtenu.

Tableau XIII
Tableau croisé du degré de compétence et du revenu obtenu

	Non (%)	Oui (%)
Inconnue	-	9,1
Très faible	33,8	31,8
Faible	35,3	13,6
Modéré	14,7	-
Élevé	16,2	45,5

*V de Cramer=0,449**; *p≤ 0,05; **p≤0,01; ***p≤0,001*

Mentionnons que nous avons croisé le type de délit et la peine obtenue, le type de délit et l'appartenance à un groupe, le type de délit et la provenance de la victime, le type de délit et la codélinquance, le type de délit et l'occupation du délinquant, la motivation et la provenance de la victime, l'appartenance à un groupe de pirates et la codélinquance, l'appartenance à un groupe de pirates et le revenu obtenu, le degré de compétence et l'occupation du cybercriminel, où aucune relation statistiquement significative n'en a résulté. Devant l'ensemble des résultats, aucune relation ne nous a semblé fallacieuse, les forces de nos relations ayant présenté des coefficients normaux.

De ces résultats, nous pouvons dégager quelques profils de délinquants. D'abord, les cyberdélinquants commettant des délits d'infiltration sont plus nombreux à présenter une motivation idéologique. Ces mêmes cyberdélinquants sont plus nombreux à avoir dans leur mire les gouvernements, il en est de même pour les délinquants motivés par l'idéologie. Dans ce même ordre d'idée, les délinquants commettant des délits d'infiltrations et ceux motivés par

l'idéologie sont moins nombreux à cibler les entreprises et les individus. D'ailleurs, les délinquants commettant les délits d'infiltrations sont moins nombreux à obtenir un revenu de leur criminalité que ceux commettant divers autres délits et les délinquants motivés par l'idéologie sont moins nombreux à être intéressés au profit de leur criminalité. Or, nous pouvons en dégager, sans généraliser, que les délinquants commettant des délits d'infiltrations seraient plus propices à avoir une motivation idéologique et à cibler les gouvernements. Mentionnons aussi que les individus motivés par le caractère idéologique de leur délit sont plus nombreux à appartenir au groupe Anonymous et LulzSec. Il est rare qu'ils n'appartiennent à aucun groupe.

Ensuite, les délinquants commettant des délits de fraudes sont plus nombreux à cibler les individus, et moins nombreux à cibler des gouvernements. Ces délinquants sont plus nombreux à être motivés par le profit et moins nombreux par l'idéologie. Dans ce même ordre d'idée, les délinquants motivés par le profit ciblent davantage les entreprises et les individus que les gouvernements. Les délinquants commettant des délits de fraudes sont plus nombreux à obtenir un revenu de leur criminalité, tout comme ceux motivés par le profit. Or, nous pouvons en déduire que les délinquants qui font de la fraude sont davantage motivés par le profit et cibleront davantage les individus et les entreprises afin d'obtenir un revenu de leur criminalité. Un élément pouvant être ajouté à ce profil est la codélinquance. Effectivement, les délinquants motivés par le profit sont plus nombreux à commettre leurs délits accompagnés d'un autre délinquant que toute autre motivation. Quant au degré de compétence, les cybercriminels motivés par le profit sont moins nombreux à avoir un degré de compétence modéré et ceux motivés par la fraude plus nombreux à avoir un degré de compétence très

faible. Toutefois, ceux obtenant un revenu sont plus nombreux à avoir un degré de compétence élevé.

Maintenant que l'échantillon a été décrit et que des relations ont pu être créées entre les variables à l'étude, il est temps de s'attaquer au noyau de ce mémoire, soit la comparaison des variables utilisées versus l'origine des cyberdélinquants. Effectivement, des tableaux de contingence en lien avec l'origine du cyberdélinquant suivront.

4.2 ANALYSES DE TABLEAUX DE CONTINGENCE EN FONCTION DE L'ORIGINE

Comme décrits dans la section de la stratégie analytique, des tableaux de contingence seront effectués afin d'observer la distribution de chacune des variables, et ce, en fonction du pays d'origine du cyberdélinquant. Ensuite, des tableaux présentant des tests statistiques plus précis de par l'ajustement Bonferroni seront réalisés et établiront s'il existe des relations significatives entre ces variables. Mentionnons que de par cet ajustement, le seuil de signification est plus difficilement atteignable. Donc, lorsqu'une relation est identifiée comme significative, il appert qu'elle est forte à tous les coups.

4.2.1 Âge des cyberdélinquants

D'abord, en ce qui a trait à l'âge moyen en fonction des territoires géographiques, un test de moyenne fut effectué. Comme la variable de l'âge présente une distribution normale, mais que le postulat voulant que chacune des catégories ait un échantillon de plus de trente cas ($N \geq 30$), un test de moyenne non paramétrique fut effectué, soit le test de Kruskal-Wallis. La région où il est le plus bas est celle de l'Europe de l'Ouest, soit d'environ 23 ans. Celle où il

est le plus élevé est l'Australasie, étant d'environ 29 ans, et ce, à échantillon égal (N=15). Le Tableau XIV inclut l'âge moyen des cybercriminels pour chacun des territoires géographiques de l'étude actuelle.

Tableau XIV

Résultat des analyses descriptives de l'âge par région

	Moyenne (x)	Mode	Écart-type (S)	N	Min	Max
Amérique du Nord	23,07	20	6,51	15	12	35
Amérique latine	25,71	20	6,23	14	19	40
Australasie	29,27	35	8,30	15	17	45
Europe de l'Ouest	23,20	19	8,33	15	16	46
Eurasie	25,13	25	3,04	15	21	32
Afrique/péninsule Arabique	25,47	19	5,69	15	19	37
total	25,30	27	6,739	89	12	46

*Khi-Deux = 8,811 ; *p≤0,05; **p≤0,01; ***p≤0,001*

Toutefois, il est possible d'observer que les cybercrimes sont perpétrés par de jeunes adultes à l'échelle internationale. Il n'existe aucune différence significative quant à la moyenne d'âge lors de laquelle le délinquant aura un attrait particulier pour ce qui est de la criminalité informatique ainsi que la commission de ces délits, et ce, en fonction de l'origine du cyberdélinquant (Khi-Deux = 8,811; $p \geq 0,05$). Il semble donc que cette moyenne d'âge soit homogène et qu'elle soit un prédicteur de la cybercriminalité, indiquant peu de variations selon les zones géographiques.

4.2.2 Pseudonymes

Comme indiqué dans la section des analyses univariées, un large écart existe dans le nombre de surnoms. Nous avons également réalisé le test de moyenne de Kruskall-Wallis pour la variable des pseudonymes afin d'avoir une meilleure idée du nombre de surnoms empruntés par les délinquants en fonction du territoire d'origine. Les délinquants en provenance d'Europe de l'Ouest ont en moyenne 1,80 surnom et ceux d'Eurasie en moyenne 2,13 surnoms, et ce, à échantillon égal (N=15). Ce sont les deux moyennes les plus élevées pour l'ensemble des six territoires géographiques. Notons que la moyenne du nombre de surnoms des délinquants en provenance d'Afrique/péninsule Arabique est de 0,80, soit la plus basse moyenne du nombre de surnoms. À titre informatif, la moyenne des surnoms pour les délinquants en provenance d'Amérique du Nord est de 1,53, celle ceux d'Amérique latine 1,00 et ceux originaires d'Australasie, 1,33. Toutefois, il n'existe aucune relation statistiquement significative en ce qui a trait au nombre de surnoms empruntés en fonction de l'origine du cyberdélinquant (Khi-Deux = 3,892; $p \geq 0,05$). Les résultats figurent dans le Tableau XV.

Tableau XV

Résultat des analyses descriptives du nombre de surnoms par région

	Moyenne (x)	Mode	Écart-type (S)	N	Min	Max
Amérique du Nord	1,53		1,552	15	0	6
Amérique latine	1		1	15	0	3
Australasie	1,33		1,345	15	0	4
Europe de l'Ouest	1,80		1,424	15	0	5
Eurasie	2,13		2,2	15	0	8

Afrique/péninsule Arabique	0,80	1,207	15	0	4
total			90		

*Khi-Deux 3,892=; *p≤0,05; **p≤0,01; ***p≤0,001*

4.2.3 Type de délit

Quant au type de délit effectué par les cyberdélinquants, il est à noter qu'il y a l'infiltration, les attaques informatiques, ainsi que la fraude qui sont représentées dans ces tests statistiques, n'ayant aucun cas de cyberpornographie et de cyberviolence dans notre échantillon. Voici le tableau récapitulatif des résultats obtenus quant au croisement de la variable du pays d'origine avec le type de délit (Tableau VXI).

Tableau XVI

Tableau croisé du type de délit selon le pays d'origine du cyberdélinquant

	Autre (%)	Infiltration (%)	Fraude (%)	Attaque (%)
Am. Nord	-	46,7	13,3	40
Am. latine	6,7	53,3	20	20
Australasie	-	66,7	26,7	6,7
Europe Ouest	6,7	80,0	-	13,3
Eurasie	-	20	20	60
Afrique/Pénin.	-	26,7	46,7	26,7

*V de Cramer= 0,338**; *p≤0,05; **p≤0,01; ***p≤0,001*

D'abord un type de délit semble se démarquer pour chacun des territoires. Pour les cyberdélinquants provenant d'Amérique du Nord, d'Amérique latine, d'Australasie et d'Europe de l'Ouest, il s'agit des délits d'infiltrations informatiques. Pour les

cyberdélinquants en provenance d'Eurasie, il s'agit des délits d'attaques informatiques. En ce qui a trait à ceux originaires d'Afrique/péninsule Arabique, il est question de délits de fraudes.

De ce tableau, il est possible de voir une surreprésentation du délit d'infiltration dans le territoire de l'Europe de l'Ouest et peu de cas en Eurasie et Afrique/péninsule Arabique. En fait, il existe quelques différences significatives quant à cette variable d'infiltration, les délinquants en faisant usage étant plus nombreux en Europe de l'Ouest (80%) qu'en Eurasie (20%) (Phi=0,600; p≤ 0,0033) et qu'en Afrique/péninsule Arabique (26,7%) (Phi=0,535; p≤0,0033) (N=30). Effectivement, l'accès à Internet est plus facile pour les délinquants en provenance d'Europe de l'Ouest et ils ont accès à de plus amples ressources technologiques.

En ce qui a trait aux délits de type frauduleux (N=30), il semble que ce soit en Afrique/Péninsule arabique qu'ils sont le plus élevés. Nous observons aussi qu'aucun délit de cette nature ne fut inscrit pour la région de l'Europe de l'Ouest. D'ailleurs, un seul résultat fut significatif quant aux tests de tableaux de contingence dichotomisés, soit qu'il existe une forte relation à l'effet que les délinquants originaires d'Afrique/péninsule Arabique (46,7%) commettront davantage de fraudes que ceux en provenance de l'Europe de l'Ouest (0%) (Phi=0,552; p≤0,0033). Ce résultat peut s'expliquer par le faible degré de compétence nécessaire à de tels types de délits, où les compétences techniques requises sont faibles, mais les compétences sociales sont importantes. Aussi, il n'est pas nécessaire d'avoir des outils technologiques développés afin de faire des délits de fraudes, ce qui correspond au territoire de l'Afrique/ péninsule Arabique. De plus, les besoins financiers diffèrent beaucoup entre ces régions, où l'Europe de l'Ouest est celle où les pays ayant un coefficient de Gini sont les plus

faibles, et l'Afrique les plus importants, donc les pays où les inégalités économiques subsistent. Ainsi, certains cyberdélinquants en provenance d'Afrique/péninsule Arabique ont possiblement des besoins financiers plus importants, donc un appât du gain plus important, les amenant à commettre des délits de fraudes.

Finalement, en ce qui concerne les attaques informatiques, la distribution du tableau permet d'observer que c'est en Eurasie qu'ils sont plus nombreux par rapport à tous les autres territoires. Un résultat s'est avéré significatif (N=30). Effectivement, les cyberdélinquants en provenance d'Eurasie (60%) commettront davantage d'attaques informatiques que ceux originaires d'Australasie (6,7%) (Phi=0,566; $p \leq 0,0033$). Ceci peut s'expliquer par le fait que les attaques informatiques ne nécessitent qu'une base d'habiletés techniques, un niveau socioéconomique faible ou modéré, puisque majoritairement, les virus informatiques seront déjà créés, il ne suffira que de les lancer.

Il est intéressant d'observer les résultats au niveau des types de délits, mais qu'en est-il de la motivation des délinquants? Y aura-t-il des résultats permettant de conclure que l'origine joue un rôle quant aux choix et motifs de ces derniers?

4.2.4 Motivation du cyberdélinquant

D'entrée de jeu, à partir de la distribution identifiée dans le Tableau XVII, il est possible de constater que les délinquants en provenance d'Afrique/péninsule Arabique sont plus nombreux à être motivés par le profit (86,7%), suivi des délinquants d'Eurasie (73,3%) et d'Amérique latine (60%). C'est toutefois en Europe de l'Ouest où il en a considérablement

moins présentant cette motivation (6,7%). Quant aux délits motivés par l'idéologie, c'est en Europe de l'Ouest (6,7%) qu'on en observe le plus et en Afrique/péninsule Arabique qu'on en observe le moins (6,7%). Pour ce qui est des autres motivations, notamment la curiosité, l'ennui et celles inconnues, il ne semble pas y avoir de grandes différences pour chacun des territoires.

Tableau XVII

Tableau croisé du type de motivation selon le pays d'origine du cyberdélinquant

	Inconnue (%)	Profit (%)	Curiosité (%)	Idéologie (%)	Ennui (%)
Am. Nord	13,3	33,3	20	13,3	20
Am. latine	6,7	60	-	33,3	-
Australasie	-	46,7	-	40	13,3
Europe Ouest	-	6,7	20	66,7	6,7
Eurasie	26,7	73,3	-	-	-
Afrique/Pénin.	6,7	86,7	-	6,7	-

*V de Cramer = 0,752***; *p≤0,05; **p≤0,01; ***p≤0,001*

Plus précisément, il existe une relation statistiquement significative, où les délinquants provenant d'Afrique/péninsule Arabique sont davantage motivés par le profit (86,7%) en comparaison avec ceux d'Europe de l'Ouest (6,7%) (N=30). Ce résultat coïncide avec celui plus haut, où la fraude représente le délit le plus prisé par ces mêmes délinquants. Toutefois, nous devrons conserver une certaine réserve quant à cette relation puisque la force est très élevée, comme en témoigne le Phi de 0,802 (p≤ 0,00007. De plus, les délinquants en provenance d'Eurasie (73,3%) sont davantage motivés par le gain financier que ceux provenant de l'Europe de l'Ouest (6,7%) (Phi=0,680; p≤ 0,00007) (N=30).

Subséquemment, il existe des relations significatives de forces élevées entre les délinquants originaires d'Europe de l'Ouest (66,7%), qui seront davantage motivés par l'idéologie que ceux d'Afrique (6,7%) (Phi = 0,623; p≤ 0,003) (N=30) et que ceux d'Eurasie (0%) (Phi=0,707; p≤ 0,0007) (N=30). Ce résultat va comme tel, dans le sens où, comme mentionné ci-haut, les délinquants d'Afrique/péninsule Arabique et d'Eurasie seront davantage motivés par le profit, comparé à ceux d'Europe de l'Ouest, ayant un accès plus facile à Internet et qui seront davantage motivés par le caractère idéologique de leurs délits.

Aucun résultat n'est significatif quant aux comparaisons des motivations de la curiosité (N=6), de l'ennui (N=6) et inconnue (N=8), et ce, au niveau international. Les motivations idéologiques (N=24) et financières (N=46) englobent une partie plutôt importante des cas de cybercriminels de l'étude actuelle, ce qui peut justifier qu'aucun résultat ne soit significatif pour les autres types de motivations, où l'échantillonnage est plus restreint. D'ailleurs, la curiosité et l'ennui peuvent aussi figurer comme des motivations plus secondaires à la commission du délit, donc être incluses ou surpassées par les autres catégories. Le Tableau XVII présente les statistiques susmentionnées.

4.2.5 Type de victime

D'emblée, à la lecture du tableau des résultats XVIII des types de victimes selon le pays d'origine du cyberdélinquant, nous pouvons constater un écart important pour les victimes gouvernementales entre l'Europe de l'Ouest et l'Eurasie. D'ailleurs, c'est le seul type de victime qui révèle une forte relation statistiquement significative (N=30). Effectivement, les victimes gouvernementales sont plus ciblées par les cyberdélinquants en provenance d'Europe

de l'Ouest (66,7%) que ceux originaires d'Eurasie (0%) (Phi=0,707; p≤ 0,0007), ce qui correspond avec la motivation idéologique pour laquelle les cyberdélinquants veulent faire paraître leurs opinions à travers les sites gouvernementaux. De plus, les gouvernements sont davantage dans la mire des cyberdélinquants en provenance d'Australasie (53,3%), en comparaison de ceux en provenance d'Eurasie (0%) (Phi=0,603; p≤ 0,003) (N=30). Le tableau XVIII présente ces résultats.

Tableau XVIII

Tableau croisé du type de victime selon le pays d'origine du cyberdélinquant

	Gouvernement (%)	Entreprise (%)	Individu (%)
Am. Nord	26,7	53,3	20
Am. latine	46,7	33,3	20
Australasie	53,3	33,3	13,3
Europe Ouest	66,7	26,7	6,7
Eurasie	-	80	20
Afrique/Pénin.	20	26,7	53,3

*V de Cramer= 0,403***; *p≤ 0,05; **p≤0,01; ***p≤0,001*

Bien qu'un seul test ait été significatif, il est intéressant d'observer la distribution de cette variable en fonction de l'origine, et ce, dans une optique exploratoire. Effectivement, le nombre de délinquants ciblant les entreprises est élevé pour les délinquants originaires d'Eurasie (80%) et il est moins élevé pour ceux en provenance d'Afrique/péninsule Arabique (26,7%). L'ajustement Bonferroni a toutefois exclu cette relation. Pour ce qui est des victimes individuelles, c'est par les cybercriminels d'Afrique/péninsule Arabique (53,3%) qu'elles semblent à première vue être plus ciblées comparé à tous les autres territoires. Également, la

distribution présente un type de victime primé par les cyberdélinquants en provenance de chacun des territoires. Pour des délinquants provenant d'Amérique du Nord et d'Eurasie, il s'agit des entreprises, pour les délinquants provenant d'Amérique latine, d'Europe de l'Ouest et d'Australasie, ce sont les gouvernements. En ce qui a trait à l'Afrique/péninsule Arabique, ce sont les victimes individuelles qui sont davantage dans leur mire.

4.2.6 Occupation du cybercriminel

De la distribution de la variable de l'occupation exposée dans le Tableau XIV, nous pouvons identifier que les délinquants en provenance d'Afrique/péninsule Arabique sont les plus nombreux à avoir une occupation inconnue, et ceux d'Europe de l'Ouest, les moins nombreux. Quant aux occupations professionnelles et éducationnelles, il ne semble pas y avoir d'écart considérable, outre que les délinquants en provenance d'Amérique du Nord (40%) et d'Eurasie (40%) semblent être ceux qui occupent davantage un emploi, lorsqu'arrêté, et ceux d'Europe de l'Ouest (40%) étant à l'école.

Dans les faits, il n'existe qu'une seule relation statistiquement significative entre l'Afrique/péninsule Arabique et l'Europe de l'Ouest (Phi=0,668; $p \leq 0,003$). En effet, c'est davantage pour les délinquants d'Afrique/péninsule Arabique que l'emploi est inconnu (86,7%) versus ceux d'Europe de l'Ouest (20%) (N=30). Cette observation peut être causée par un manque d'information au niveau médiatique. Il est plus facile et intéressant de relater les cas où l'emploi du cybercriminel était en lien avec sa criminalité, soit qu'il occupait un emploi en sécurité informatique, comme certains en Europe de l'Ouest, qu'un cas où l'emploi n'était pas en lien avec son crime, ou s'il n'avait tout simplement aucun emploi important,

comme ceux provenant d'Afrique/péninsule Arabique. L'information a par conséquent possiblement été perdue ou filtrée. Le Tableau XIV présente la dispersion des résultats pour le type d'occupation selon le pays d'origine du cyberdélinquant.

Tableau XIV

Tableau croisé du type d'occupation selon le pays d'origine du cyberdélinquant

	Inconnue(%)	Professionnelle(%)	Éducationnelle(%)	Autre(%)
Am. Nord	40	40	13,3	6,7
Am. latine	66,7	26,7	6,7	-
Australasie	40	46,7	6,7	6,7
Europe Ouest	20	26,7	40	13,3
Eurasie	60	40	-	-
Afrique/Pénin.	86,7	6,7	6,7	-

*V de Cramer = 0,582**;*p≤0,05; **p≤0,01; ***p≤0,001*

4.2.7 Provenance de la victime

Pour cette variable, la distribution révèle qu'il ne semble pas y avoir beaucoup de différences d'un territoire à l'autre, outre pour ce qui est des victimes en provenance de l'Amérique du Nord (Tableau XV). Effectivement, il existe une forte relation significative entre les cyberdélinquants originaires d'Amérique du Nord et d'Australasie (Phi=0,586; p≤0,003), soit que ceux provenant d'Amérique du Nord visent majoritairement les victimes de cette même région (80%) en différence avec ceux en provenance de l'Australasie (21,4%) et de l'Afrique (15,4%) (Phi = 0,645; p≤ 0,003). Aucun résultat significatif n'a découlé des tests de tableaux de contingence pour les victimes en provenance du monde, de l'Eurasie, de l'Europe de l'Ouest, de l'Amérique latine et de l'Afrique/péninsule Arabique. Le tableau suivant rapporte ces résultats.

Tableau XV

Tableau croisé de la provenance de la victime selon le pays d'origine du cyberdélinquant

	Am.Nord	Am.latine	Austral	EuroOuest	Eurasie	Afrique	Monde
Am. Nord	73,3	-	-	-	-	-	26,7
Am. latine	33,3	46,7	-	-	-	-	20
Australasie	21,4	-	64,3	-	-	-	14,3
Europe Ouest	53,3	-	-	20	-	-	26,7
Eurasie	72,7	-	9,1	-	9,1	-	9,1
Afrique/Pénin.	15,4	-	15,4	-	-	46,2	23,1

*V de Cramer= 1,233***;*p≤0,05; **p≤0,01; ***p≤0,001*

4.2.8 Revenu obtenu

D'abord, soulignons qu'il y a un faible échantillon quant aux délinquants ayant obtenu un revenu de leur criminalité (N=22). À partir de la distribution obtenue par le croisement des variables (Tableau XVI), nous observons que les délinquants en provenance d'Afrique/péninsule Arabique sont ceux qui obtiennent davantage de revenus (53.3%), suivis des délinquants provenant d'Eurasie (26,7%) et d'Amérique latine (26,7%). Ce sont les délinquants en provenance d'Australasie qui en obtienne le moins (0%).

À cet effet, une forte relation s'est avérée significative (Phi= 0,655; p p≤0,003), soit que les cybercriminels d'Afrique/péninsule Arabique (60%) sont plus nombreux à obtenir un revenu de leur criminalité informatique que ceux d'Australasie (0%) (N=30). Ce résultat correspond à celui de la motivation principale des délinquants d'Afrique/péninsule Arabique susmentionnée, soit le profit, ainsi que le type de délit primé, soit les délits frauduleux.

Tableau XVI

Tableau croisé du revenu obtenu en fonction du pays d'origine du cyberdélinquant

	Non (%)	Oui (%)
Am. Nord	80	20
Am. latine	73,3	26,7
Australasie	100	0
Europe Ouest	80	20
Eurasie	73,3	26,7
Afrique/Pénin.	46,7	53,3

V de Cramer= 0,366; *p≤0,05; **p≤0,01; ***p≤0,001*

Ces résultats sont inévitablement en lien avec la différence au niveau des revenus par habitant de ces unités géographiques. Effectivement, comme les inégalités entre les revenus des habitants provenant de l'Afrique/péninsule Arabique sont plus élevées, selon le coefficient de Gini, il est plus probable qu'un cyberdélinquant commette des délits dans le but d'obtenir un revenu de ceux-ci. Inversement, les pays d'Australasie qui ont un coefficient de Gini plus faible, ne semblent pas souffrir de déficience économique, où la motivation des criminels diverge de celle en provenance d'Afrique, donc où le revenu ne sera pas directement en lien avec leur criminalité.

En référence à l'étude de l'écart plutôt important entre le revenu minimum (3 730$) et le revenu maximum (1 million $), il est possible d'avancer qu'il est justifié par l'origine des délinquants. Effectivement, celui ayant eu un revenu de 1 million de dollars, âgé de 29 ans et en provenance d'Europe de l'Ouest, avait un degré de compétence élevé et a fraudé des millions de numéros d'identifications personnelles d'individus de par des attaques informatiques importantes. Ce territoire géographique est situé dans ceux ayant un accès facile à Internet, ainsi qu'un niveau économique élevé. Pour ceux ayant obtenu un revenu de 3 730$,

ils sont en provenance d'Afrique/péninsule Arabique, âgés de 34 et 37 ans, et ont commis des délits d'hameçonnage dans le but d'obtenir des mots de passe Internet de sites bancaires.

4.2.9 Appartenance à un groupe

En ce qui a trait à l'appartenance à un groupe de cybercriminels, aucune différence significative ne fut relevée au niveau des différentes origines des délinquants informatiques, ce qui peut s'expliquer par le faible échantillonnage de cas appartenant à un groupe (N=35). Toutefois, si nous considérons la distribution exposée au Tableau XVII, il semble que ce soit les délinquants en provenance d'Europe de l'Ouest qui sont plus nombreux à appartenir au groupe LulzSec (33,3%), et ce, en comparaison de tous les autres territoires.

Tableau XVII
Tableau croisé de l'appartenance à un groupe selon le pays d'origine du cyberdélinquant

	Autre(%)	Anonymous(%)	LulzSec(%)	Aucun(%)
Am. Nord	6,7	13,3	13,3	66,7
Am. latine	13,3	26,7	-	60
Australasie	6,7	26,7	6,7	60
Europe Ouest	6,7	6,7	33,3	53,3
Eurasie	-	-	-	100
Afrique/Pénin.	6,7	-	-	93,3
	*V de Cramer= 0,574**; p≤0,05; **p≤0,01; ***p≤0,001*			

4.2.10 Présence de trouble de santé mentale

Il en est de même quant à la présence d'un trouble de santé mentale. Aucune différence significative entre les différents territoires géographiques ne fut obtenue suite aux tests de tableaux croisés, la distribution identifiée au Tableau XVIII n'étant également pas révélatrice. Encore une fois, il est possible que ce soit en lien avec le faible échantillon de délinquants présentant un trouble de santé mentale relevé lors de la collecte de données (N=18).

Tableau XVIII
Présence d'un problème de santé mentale selon le pays d'origine du cyberdélinquant

	Non (%)	Oui (%)
Am. Nord	80	20
Am. latine	86,6	13,3
Australasie	93,3	6,7
Europe Ouest	80	20
Eurasie	100	-
Afrique/Pénin.	100	-

*V de Cramer = 0,280; *p≤0,05; **p≤0,01; ***p≤0,001*

Compte tenu de l'ajustement Bonferroni, les chances étaient davantage réduites à ce que des résultats soient significatifs. Le fait qu'aucun résultat ne le soit nous laisse croire en l'absence de différence territoriale à l'échelle internationale quant à l'appartenance à un groupe et les troubles de santé mentale. Cependant, un plus large échantillon permettrait d'affirmer que cette variable n'est pas prédictrice de la cybercriminalité avec plus de certitude, mais compte tenu du peu de cas recueillis, il n'est pas possible de s'avancer davantage à ce niveau.

4.2.11 Codélinquance

La codélinquance n'est pas une variable pour laquelle il y aura une variation d'un territoire géographique à l'autre, n'ayant obtenu aucun résultat significatif de ces croisements. Comme les forums, les communautés et les plateformes informatiques sont accessibles à tous, et ce, à travers le monde, il est juste d'observer qu'effectivement, aucune différence significative n'existe entre les différentes régions. Rapidement, nous constatons de la distribution que ce sont les délinquants en provenance d'Afrique/péninsule Arabique (86,7%) et ceux en provenance d'Amérique latine (86,7%) qui semblent davantage commettre leurs délits accompagnés et ceux d'Amérique du Nord qui le sont le moins (46,7%).

Tableau XIX

Tableau croisé de la codélinquance en fonction du pays d'origine du cyberdélinquant

	Non (%)	Oui (%)
Am. Nord	53,3	46,7
Am. latine	13,3	86,7
Australasie	33,3	66,7
Europe Ouest	40	60
Eurasie	46,7	53,3
Afrique/Pénin.	13,3	86,7

*V de Cramer= 0,327; *p≤ 0,05; **p≤0,01; ***p≤0,001*

4.2.12 Degré de compétence du cyberdélinquant

D'abord, le Tableau XX présente les pourcentages de la distribution des divers degrés de compétences en fonction du territoire d'origine du cyberdélinquant. Ces derniers résultent des premiers tests de tableaux croisés, effectués entre la variable de l'origine et du degré de compétence.

Tableau XX

Tableau croisé du degré de compétence du cyberdélinquant en fonction de son pays d'origine

	Inconnu (%)	Très faible (%)	Faible (%)	Modéré (%)	Élevé (%)
Am. Nord	-	6,7	33,3	20	40
Am. latine	-	46,7	33,3	6,7	13,3
Australasie	-	-	66,7	20	13,3
Europe Ouest	-	46,7	20	13,3	20
Eurasie	-	40	20	6,7	33,3
Afrique/Pénin.	13,3	60	6,7	0	20

*V de Cramer = 0,342**; *p≤ 0,05; **p≤0,01; ***p≤0,001*

Il est possible d'observer des écarts qui semblent importants entre divers territoires. Effectivement, nous pouvons observer que les délinquants en provenance d'Afrique/péninsule Arabique sont plus nombreux à avoir un très faible degré de compétence (60%) et les délinquants originaires d'Australasie un faible degré de compétence (66,7%). Pour ce qui est

des degrés de compétence modéré et élevé, il ne semble pas y avoir de différences importantes, les délinquants provenant d'Europe de l'Ouest plus nombreux à présenter un degré de compétence modéré et ceux d'Amérique du Nord, un degré de compétence élevé. Le tableau XX présente ces résultats.

Suite aux tests de tableaux de contingence avec les variables dichotomisées et l'ajustement Bonferroni, quelques résultats se sont avérés significatifs en ce qui a trait au degré de compétence du délinquant. D'abord, quelques résultats sont observés au niveau des cyberdélinquants ayant un degré de compétence très faible, soit ceux ayant des habiletés informatiques suffisamment de base et modestes pour que les activités délictuelles soient accessibles à tout individu. Les cyberdélinquants en provenance d'Afrique/péninsule Arabique sont plus nombreux à avoir un très faible degré de compétence (60%) que les délinquants en originaires d'Amérique du Nord (6,7%) (Phi= 0,566; $p \leq 0,003$) ainsi que ceux provenant d'Australasie (0%) (Phi= 0,655; $p \leq 0,00007$). En d'autres mots, l'absence de compétence semble plus répandue parmi les délinquants d'Afrique/péninsule Arabique. Ensuite, les cyberdélinquants provenant d'Europe de l'Ouest (46,7%; Phi= 0,552; $p \leq 0,003$), ceux venant d'Amérique latine (46,7%; Phi= 0,552; $p \leq 0,003$) ainsi que ceux originaires d'Eurasie (46,7%; Phi= 0,552; $p \leq 0,003$) sont significativement plus nombreux à présenter un très faible degré de compétence, versus ceux d'Australasie (0%).

Un seul résultat est significatif au niveau du degré de compétence faible des cyberdélinquants, soit que les cyberdélinquants en provenance d'Australasie (66,7%) sont plus enclins à représenter un degré de compétence faible que ceux d'Afrique/péninsule Arabique

(6,7%; Phi= 0,623; p≤0,003), territoire où c'est le très faible degré de compétence qui était significatif.

Ces résultats suggèrent donc que les délinquants d'Amérique du Nord et d'Australasie sont davantage compétents, et ce, possiblement compte tenu de l'accès plus facile aux ressources informatiques, à l'équipement technologique, tout comme l'accès plus rapide à Internet. D'autre part, le fait qu'ils s'expriment également en anglais et que cela leur donne accès à plus de ressources d'apprentissage peut aussi être une des raisons de cette différence.

4.2.13 Sentence obtenue

Comme indiqué dans la section des analyses univariées, il ne faut pas perdre de vue que les cas de notre base de données sont recueillis d'articles de médias, donc représentant des délits importants qui risquent fortement d'être judiciarisés. Toutefois, l'analyse demeure intéressante et la distribution de la variable est présentée dans le Tableau XXI.

Tableau XXI
Tableau croisé de la sentence obtenue en fonction du pays d'origine du cyberdélinquant

	Aucune (%)	Amende/Travaux compensatoires(%)	Peine privative et probation(%)	Amende et peine privative(%)	Inconnue(%)
Am. Nord	6,7	6,7	40	33,3	13,3
Am. latine	-	-	13,3	26,7	60
Australasie	26,7	-	-	46,7	26,7
Europe Ouest	20	13,3	53,3	13,3	0
Eurasie	26,7	-	40	20	13,3
Afrique/Pénin.	-	-	13,3	13,3	73,3

D'abord, en survolant ces résultats, nous pouvons observer que c'est en Europe de l'Ouest (53,3%) où il y a davantage de peines privatives de liberté et de sentences de probation

et en Australasie (0%) où il y en a le moins. Quant aux amendes et peines privatives de liberté, elles semblent être davantage octroyées aux délinquants provenant d'Australasie (46,7%) et à ceux originaires d'Amérique du Nord (33,3%).

Ensuite, quelques résultats furent significatifs suite aux analyses des tableaux de contingence avec l'ajustement Bonferroni. L'échantillon pour chacun de ces croisements est de N=30. D'abord, les délinquants en provenance d'Europe de l'Ouest (53,3%) obtiennent davantage une peine privative de liberté et une peine de probation que ceux en provenance d'Australasie (0%) (Phi = 0,603; $p \leq 0,003$). Quant aux autres résultats, ils sont en lien avec la sentence inconnue des cas de cyberdélinquants. Or, les sentences des délinquants en provenance d'Afrique/péninsule Arabique (73,3%), sont davantage inconnues que celles d'Amérique du Nord (13,3%) (Phi = 0,605; $p \leq 0,003$) (N=30), d'Europe de l'Ouest (0%) (Phi = 0,761; $p \leq 0,00007$) ainsi que d'Eurasie (13,3%) (Phi = 0,605; $p \leq 0,003$). Finalement, les peines obtenues pour les délinquants originaires d'Amérique latine (60%) sont plus inconnues que celles des délinquants provenant d'Europe de l'Ouest (0%) (Phi = 0,655; $p \leq 0,003$).

En définitive, ces tests de tableaux croisés nous ont permis d'établir les différences significatives des caractéristiques personnelles et délictuelles des cyberdélinquants et seront globalement discutés dans la section de l'interprétation des résultats.

Toutefois, voici un récapitulatif des caractéristiques spécifiques pour certaines régions et où se trouvent les différences les plus significatives. Nous allons effectuer un portrait de ces résultats, sans toutefois rapporter toutes les comparaisons aux autres pays qui sont déjà susmentionnées. Les délinquants originaires d'Europe de l'Ouest présentent des résultats

supérieurs en ce qui a trait aux délits d'infiltrations, à la motivation idéologique, aux victimes gouvernementales, au très faible degré de compétence ainsi qu'à la peine privative de liberté. Les délinquants en provenance d'Eurasie seraient plus nombreux à utiliser les délits d'attaques informatiques, motivés par le profit et présentant un très faible degré de compétence. Les délinquants provenant de l'Afrique/péninsule Arabique présentent des différences significatives en ce qui a trait aux délits frauduleux, obtenant un revenu de leur criminalité, étant motivés par le profit, présentant un emploi inconnu et un très faible degré de compétence. Toujours en ce qui a trait aux délinquants de ce territoire, une différence significative subsistait au niveau de la sentence, qui semble plus inconnue que plusieurs autres territoires. En ce qui a trait aux territoires de l'Amérique du Nord, aucune caractéristique plus significative que les délinquants en provenance d'un autre territoire ne furent obtenus. Il en est de même pour les délinquants d'Amérique centrale, quoiqu'ils présentent une différence significative au niveau du degré de compétence très faible. Quant aux délinquants en provenance d'Australasie, ils présentent une différence en ce qui concerne le type de victime, soit les gouvernements, ainsi que le faible degré de compétence.

CHAPITRE 5 : INTERPRÉTATION DES RÉSULTATS

Plusieurs liens furent créés suite à la présentation des résultats dans le chapitre précédent. Cependant, il est important de faire un résumé de ces analyses et de les interpréter globalement en fonction des profils observés ainsi que des caractéristiques pouvant entrainer les différences territoriales entre ces derniers, notamment l'impact de la vitesse Internet, la motivation selon l'origine et les inégalités financières des cyberdélinquants. Ainsi, les analyses seront articulées autour de ces caractéristiques. D'abord, une interprétation globale sera effectuée, suivie d'une interprétation en fonction des profils principaux des cyberdélinquants, soit en lien avec les motivations du profit et ensuite de l'idéologie.

5.1 Interprétation globale

D'entrée de jeu, les résultats des variables démographiques de l'étude actuelle ne sont pas bien différents de ceux des précédentes études portant sur la cyberdélinquance. Effectivement, il est possible d'affirmer que la cyberdélinquance est davantage perpétrée par des hommes, confirmant ici les études de Yar (2005), Dupont (2012), Schell (2007), Woo (2003) ainsi que Moon, McCluskey et McCluskey (2010). Ces cyberdélinquants sont en moyenne âgés de 25 ans, moyenne plus élevée que l'étude de Holt et Schell (2011), pour laquelle elle était évaluée à 18 ans. La mi-vingtaine est relevée comme étant normalement l'âge de décrochage des cybercriminels (Hollinger 1991; Yar, 2005) et non celui de la commission des délits. Or, l'âge moyen de la base de données actuelle est plutôt élevé, ce qui peut s'expliquer par le fait que celle-ci est formée de délinquants informatiques ayant été arrêtés, médiatisés et qui n'étaient probablement pas tous à leur première offense. Effectivement, plusieurs de ces derniers sont réputés comme d'importants pirates informatiques dont le crime fut médiatisé de par leur

grande notoriété, tels Darren Martyn, Albert Gonzalez, Gary McNikkon, Noor Uddin Aziz, Jeremy Hammond, etc. Ainsi, comme la base de données s'inspire d'arrestations médiatisées, il est plus probable que cette moyenne d'âge soit davantage élevée et donc moins représentative.

Au niveau de la sphère sociale, les résultats permettent de conclure que le phénomène de la cyberdélinquance est une criminalité pour laquelle le délinquant sera accompagné en moyenne d'un autre individu. Par ailleurs, comme nous avions pour objectif de cibler les différences au niveau international, nous constatons qu'aucune différence significative n'existe entre les divers territoires géographiques à ce niveau. Nous pouvons expliquer cela par l'existence des réseaux sociaux, des plateformes informatiques et de multiples forums accessibles aux délinquants informatiques. Effectivement, comme peu de délinquants sont associés à des groupes criminels et qu'ils auraient un réseau social plus limité, ils compensent en communiquant par des moyens dépersonnalisant, soit par l'intermédiaire de leur ordinateur sur des forums. Il est intéressant de constater que cela se reflète dans leurs associations et actions. Sur une base commune à l'échelle mondiale, l'ordinateur et Internet sont nécessaires pour la commission du délit informatique tout comme une motivation intrinsèque est essentielle, favorisant ainsi l'accès au monde virtuel. Ceci offre la possibilité aux délinquants présentant les habiletés et techniques nécessaires de s'associer avec un individu connu par l'intermédiaire de ces réseaux et d'agir conjointement. Il y aura conséquemment présence de participation mutuelle et d'association mutuelle (Holt, 2009). Nous émettons donc l'hypothèse qu'il est plus facile de s'associer à quelqu'un présentant les mêmes intérêts et objectifs, compte tenu de l'ampleur et de l'étendue de leurs communautés informatiques, sans toutefois ressentir le besoin de se joindre à un groupe de grande envergure. Toutefois, l'origine du cyberdélinquant

n'aura aucune influence en fonction des sociétés sur l'association entre pairs délinquants, contrairement à ce que Best et Luckenbill (1994) avaient relevé, soit que l'origine du cyberdélinquant aurait une influence au niveau de cette association. Cette différence aurait pu s'expliquer par le type de crime analysé, mais aucune relation n'est non plus identifiée quant au croisement des variables du type de crime et de la codélinquance.

Pour la suite, voici un rappel des différentes variables les plus populaires. Quant au type de délit, c'est d'abord l'infiltration qui prime (48,9%), suivie des attaques informatiques (27,8%) qui sont suivies de près par la fraude (21,1%). Concernant la motivation du cyberdélinquant, elle est d'abord en lien avec le profit acquis de la criminalité (51,1%), suivi du caractère idéologique de leurs actions (25,6%). En ce qui a trait aux victimes les plus ciblées, ce sont d'abord les entreprises/banques (44,2%), suivies des gouvernements/écoles (35,6%) et ensuite, des individus (22,2%). D'ailleurs, ce dernier résultat est équivalent à celui de l'étude d'Hollinger (1991), où les criminels informatiques sont davantage attirés par les grandes entreprises, plutôt que les individus. En fait, un biais peut ici être relevé puisque notre base de données fut complétée suite aux arrestations médiatisées, donc fort possiblement pour les affaires plus sérieuses et laborieuses, ce qui conséquemment résulte en des types de victimes de plus grande envergure. Malgré tout, des liens et associations seront effectués entre ces différentes variables.

5.2 Interprétation en fonction du profit

De prime abord, le premier profil type des cyberdélinquants que nous interpréterons est celui en lien avec le profit, celui où ils sont motivés par l'appât du gain et commettront un

délit pour assouvir leurs besoins financiers. Pour ce profil, et de par les résultats obtenus lors des croisements de ces variables, il est possible d'observer une ligne d'articulation entre les différentes variables, soit la motivation, le type de victime et le type du délit perpétré par les délinquants informatiques. En effet, comme susmentionnés, les cyberdélinquants sont principalement motivés par le profit acquis de leur criminalité. Cette source première de motivation des délinquants informatiques concorde avec le type de victime la plus ciblée par ceux-ci, soit les entreprises/banques. D'ailleurs, les délinquants motivés par le profit sont moins propices à viser les gouvernements. Les victimes corporatives sont plus à risque de fraude et de délits acquisitifs compte tenu de l'ampleur des avoirs financiers des entreprises, comparées à un individu chez qui ils seront moins attrayants. Le délit concordant à une motivation pécuniaire et à des victimes potentielles de grande envergure est sans aucun doute la fraude, ce qui fut constaté lors du croisement des variables. Effectivement, cette motivation se reflète sur le mode opératoire qu'ils choisiront, l'infiltration était négativement reliée avec le profit. L'objectif de ce mémoire est de constater s'il existe des différences au plan international, donc un parallèle sera effectué avec la provenance des pirates correspondant à ce profil.

Le profil selon lequel les délinquants en provenance des pays en développement où des inégalités entre les revenus persistent sont motivés par des délits en lien avec l'argent, telle la fraude, s'est réellement dessiné. Effectivement, les délinquants informatiques en provenance de l'Afrique/péninsule Arabique et d'Eurasie seront davantage motivés par le profit de leur criminalité que ceux en provenance d'Europe de l'Ouest. D'autre part, la fraude est un prédicteur des délinquants originaires d'Afrique/péninsule Arabique, lesquels commettront

davantage de fraudes que ceux d'Europe de l'Ouest. Certaines caractéristiques spécifiques à ces régions peuvent expliquer ce profil plus typique de cyberdélinquants, notamment le coefficient Gini plus élevé qui peut expliquer le sentiment d'injustice vécu par ces criminels ainsi que leur justification du délit, soit d'aller rechercher de l'argent ailleurs. En se référant au coefficient de Gini, il est possible d'observer que c'est en Europe de l'Ouest où il persiste le plus d'équités dans les revenus des habitants, et que c'est majoritairement de l'Afrique/péninsule Arabique que les inégalités salariales persistent le plus. De plus, les opportunités économiques sont effectivement réduites, versus l'Europe de l'Ouest, pays industrialisé ayant de meilleures opportunités financières. Ceci pourrait expliquer leur attrait pour l'argent.

Également, ceci peut s'expliquer par l'accès à Internet et sa vitesse limitée. En effet, cet élément influencera le mode opératoire du délinquant originaire de régions plus limitées, en entraînant un choix de criminalité différent de ceux des régions où Internet est le mode de communication le plus prisé puisque la complexité du crime informatique se trouve affectée par ce manque de ressource, tout comme le peu d'efficacité de celles-ci. Non seulement la vitesse Internet d'Afrique/péninsule Arabique figure dans les moins rapides, mais l'Afrique et les États Arabes représentent les pays où les ménages ont le moins d'ordinateurs, le moins accès à Internet et où il y a le moins d'utilisation d'Internet. Conséquemment, cette faiblesse au niveau de la vitesse Internet ainsi que de l'accès aux ressources technologiques peut expliquer la tendance à perpétrer des crimes frauduleux, étant plus faciles et accessibles aux délinquants en provenance de ces territoires, et ce, dans le but d'obtenir un certain profit de la criminalité. Ce manque de ressource, donc le manque d'opportunités et de circonstances,

aurait pour effet de réduire leurs chances de développer un degré de compétence suffisant pour perpétrer des délits de plus grande ampleur. La sphère des habiletés techniques, la capacité de savoir-faire, de manipulation et de prise de contact avec les individus sera de ce fait plus importante que celles en lien avec la sphère des connaissances dont ils feront preuve, et ce, par exemple dans le but de commettre de l'hameçonnage et de parvenir à soutirer de l'argent de leurs victimes.

Subséquemment, les cybercriminels en provenance d'Afrique/péninsule Arabique sont plus nombreux à obtenir un revenu de la criminalité, soit par exemple en comparaison de ceux d'Australasie. Effectivement, à l'aide de la base de données actuelle, il est possible d'observer que 0% des cyberdélinquants en provenance d'Australasie ont obtenu un revenu, comparé à 53.3% des cyberdélinquants en provenance d'Afrique/péninsule Arabique. Cet attrait pour l'obtention d'un revenu serait motivé par l'appât du gain contrairement à ceux d'Australasie où les inégalités financières sont moins importantes. D'ailleurs, d'autres résultats solidifient cette relation, notamment ceux où les délinquants motivés par le profit sont ceux qui sont plus nombreux à obtenir un revenu de leur criminalité, tout comme les délinquants commettant des délits de fraudes.

Dans ce même ordre d'idée, les délinquants en provenance d'Afrique/péninsule Arabique ciblent davantage des individus que des entreprises et des gouvernements. Effectivement, compte tenu du peu de moyens technologiques et d'un très faible degré de compétence, il est plus facile d'attaquer des individus de par leur vulnérabilité ou le peu d'outils de prévention mis à leur disposition. D'ailleurs, les délinquants commettant des délits de fraudes ciblent

davantage les individus que ceux présentant une autre motivation. Selon les cas tirés de notre base de données, les délinquants en provenance de ce territoire (N=15) tenteront d'attirer leur sympathie en faisant de l'hameçonnage, et obtiendront certaines données bancaires frauduleusement (46,7%). Penons par exemple les cyberdélinquants Evans Ukah Mendi et William Tambo, qui ont créé une fausse page de compte bancaire afin de voler les mots de passes des utilisateurs. Ils envoyaient aussi des pourriels et lorsque le destinataire de leurs courriels répondait à l'un d'eux, leurs données personnelles, y compris les mots de passe, étaient piratées. Les dommages causés par ces derniers s'élèvent à environ 27 100$ US.

Quant aux délinquants en provenance d'Eurasie, ils sont davantage motivés par le profit. Comme il est susmentionné, les délinquants motivés par le profit sont plus à même de s'en prendre aux entreprises que les délinquants présentant toute autre motivation. Or, nous pouvons établir que les délinquants en provenance d'Eurasie, motivés par le profit, auront possiblement dans leur mire les entreprises. Prenons par exemple le délinquant Aleksander Survorov, provenant d'Estonie, ayant volé 240 000 numéros de cartes de crédit. Ce pirate «victimize businesses and individuals, posing a serious threat to their financial security» (Justice News, 2012). Vladimir Levin, provenant de Russie, en est aussi un cas typique, lequel a fraudé le système de transaction du compte Citibank afin de faire des transactions illégales à travers plusieurs pays. Prenons aussi comme exemple Dmitry Zubakha, originaire de Russie et qui a fraudé les grands sites corporatifs d'Amazone et Ebay, volant plus de 28 000 numéros de cartes de crédits. Peu de délinquants d'Afrique/péninsule Arabique portaient des alias lors de leur arrestation, de par leur criminalité davantage frauduleuse, par exemple l'utilisation d'hameçonnage. Il ne leur est à ce moment pas nécessaire de porter plusieurs surnoms, ces

cybercriminels étant peu impliqués dans les communautés informatiques et ayant un degré de compétence moins élevé.

Finalement, nous nous attendions à ce que les délinquants en provenance d'Amérique latine correspondent au profil de la motivation en lien avec le profit, ce qui n'est pas le cas. En fait, très peu de résultats ont été obtenus en lien avec ce territoire, possiblement en lien avec la taille de l'échantillon. Dans les faits, il ne s'est pas particulièrement démarqué des autres territoires où des différences plus significatives persistent au niveau économique, tel le territoire de l'Afrique/péninsule Arabique. Comme le Brésil est exclu de ce mémoire, étant une de nos limites, il y aura possiblement eu un effet pervers dans la recherche.

En résumé, il est possible d'identifier certains schèmes pour les pays où la vitesse d'Internet est plus faible, où l'accès aux ressources technologiques est limité et où des inégalités entre les revenus subsistent. Les délinquants d'Afrique/péninsule Arabique sont davantage motivés par le profit (86,7%) et commettent davantage de délits frauduleux (46,7%) en ciblant des individus (53,3%) dans le but d'obtenir un revenu (53,3%), de par un manque de ressources. Les statistiques correspondent à la proportion des délinquants pour ce territoire présentant ces caractéristiques. Quant aux délinquants d'Eurasie, toujours en comparaison des autres territoires géographiques à l'étude, ils sont davantage motivés par le profit (73,3%), et utiliseront les attaques informatiques (60%) afin d'y parvenir. Nous pouvons également constater que la motivation correspondant à ce profil est de nature extrinsèque, soit dans le but de retirer des bénéfices.

5.3 Interprétation en fonction de la motivation idéologique

Ensuite, le deuxième profil type des cyberdélinquants que nous traduirons est celui en lien avec la motivation idéologique. Comme pour le premier profil type, nous avons constaté qu'un fil conducteur existe entre les différentes variables à l'étude. La motivation idéologique ou politique des cybercriminels, la seconde motivation la plus importante mondialement, peut être mise en lien avec le deuxième type de victime le plus visé, soit les gouvernements. En réponse au croisement de ces variables, nous avons pu observer une relation. Effectivement, les délinquants motivés par l'idéologie sont plus nombreux à cibler les gouvernements, et moins nombreux que ceux présentant une autre motivation à cibler les entreprises et les individus. Afin de faire valoir leur point de vue et de faire entendre leur mécontentement, ces délinquants utiliseront davantage l'infiltration comme mode opératoire. Il est intéressant de constater que ce sont les délinquants en provenance de ce territoire qui utilisent davantage de pseudonymes. Ryan Ackroyd, portant cinq (5) surnoms et ayant une criminalité d'infiltrations informatiques, le pirate informatique Darren Martyn, portant quatre (4) surnoms et infiltrant des instances gouvernementales tout comme Lauri Love, dénombrant quatre (4) identités. Les délinquants en provenance d'Europe de l'Ouest portent davantage de surnoms compte tenu de l'ampleur de leur criminalité, soit les délits d'infiltrations. En revanche, certains cybercriminels qui commettent des délits frauduleux, des infiltrations anonymes ou de l'hameçonnage, ce qui ne requiert préalablement aucun surnom puisque l'identité, excepté s'ils se font arrêter, ne devrait pas être dévoilée.

Par ailleurs, ces liens peuvent être expliqués par certaines caractéristiques, notamment celles selon lesquelles les cyberdélinquants homologues à ce profil seraient originaires d'une

région où l'accès à Internet est facile et où il existe des conflits armés ou des mouvements sociaux très actifs. Les territoires ayant été ciblés pour la facilité d'accès à l'Internet sont l'Europe de l'Ouest et l'Amérique de Nord. Pour les conflits armés, le territoire de l'Eurasie fut plus spécifiquement ciblé.

D'abord, c'est en Europe de l'Ouest où nous observons le plus de délinquants motivés par l'idéologie (66,7%), où l'infiltration (80%) est prisée pour arriver à leurs fins, et ce, encore plus qu'en Eurasie (0%; 20%). Effectivement, nous avons pu constater que les délinquants utilisant le mode opératoire des délits intrusifs sont davantage motivés par le caractère idéologique de leurs actions que ceux perpétrant d'autres types de délits, et sont encore moins motivés par le profit. Par exemple, un cybercriminel en provenance de l'Europe de l'Ouest, Gary McKinnon avait comme motivation la protection de l'environnement. Quant au pirate informatique Donncha O'Cearbhaill, il est un activiste socialiste qui avait commis son délit dans le but de rendre les informations publiques et les documents du gouvernement en encourageant la propension de ces informations.

Ce profil de cyberdélinquance peut s'expliquer par un accès plus facile à l'équipement informatique, ce qui leur permet de perpétrer des délits de plus grande envergure. Effectivement, c'est en Europe de l'Ouest où l'accès à Internet est le plus élevé et où le taux des individus faisant usage d'Internet est très élevé (Union des télécommunications, 2014). Quant à la vitesse d'Internet, l'Europe de l'Ouest fait partie des territoires les plus rapides (Akamai, 2013). Ainsi, le délit informatique pour lequel la facilité d'accès tout comme la vitesse d'Internet sont primordiales, afin que le tout se déroule dans la rapidité et dans

l'efficacité, est bien l'infiltration. De plus, la sphère des connaissances en lien avec le degré de compétence nécessaire à ce type de délit est plus importante, et c'est grâce aux avantages de l'accès aux ressources que les délinquants de ce territoire peuvent acquérir les habiletés techniques à la perpétration de tels délits.

Subséquemment, un lien intéressant peut être formulé, c'est-à-dire que les délinquants d'Europe de l'Ouest cibleront les gouvernements. D'ailleurs, suite au croisement entre les variables, nous pouvons observer que les cyberdélinquants commettant des délits de type intrusifs sont ceux qui visent le plus les gouvernements tout comme ils sont ceux qui ciblent le moins les entreprises et les individus. Prenons pour exemple le cyberdélinquant Jake Leslie Davis, 17 ans, ayant infiltré les systèmes de la CIA et du FBI avec comme motivation la passion pour le changement. Non seulement leur motivation et le type de criminalité concordent, mais les victimes aussi. En effet, pour ces délits où l'idéologie prime, donc pour lesquels le désir de se faire entendre ou de manifester un désaccord est essentiel, la victime la plus à risque à ce moment d'être dans la mire de ces criminels est bel et bien une instance gouvernementale. Les délinquants en provenance d'Europe de l'Ouest cibleront davantage ce type de victime que ceux d'Europe de l'Est. Dans ce même ordre d'idée, suite au croisement des variables de la motivation et de l'appartenance à un groupe, nous avons obtenu quelques conclusions intéressantes qui renchérissent ce profil. En effet, les délinquants motivés par l'idéologie sont plus nombreux à faire partie des groupes Anonymous et LulzSec que ceux présentant une autre motivation, tout comme ils sont les moins nombreux à n'appartenir à aucun groupe. L'appartenance des délinquants affiliés représente le désir de ces

cyberdélinquants à faire valoir leur opinion par l'intermédiaire de ce groupe, puisque leur message sera affiché à plus grande échelle et que celui-ci sera soutenu par des pairs

En résumé, les schèmes identifiables au niveau de ce type de motivation sont : en Europe de l'Ouest, la motivation idéologique mène les délinquants à infiltrer les sites gouvernementaux, et ce, dans le but de faire passer des messages. Prenons pour exemple Per Gottfrid Svartholm Warg, âgé de 29 ans et en provenance de Suède, qui invoquait la liberté de parole par les plateformes telle PirateBay, ainsi que Damien, âgé de 17 ans et originaire d'Yvelines, qui faisait usage de piraterie informatique dans le but de faire passer des messages en remplaçant des pages d'accueil de sites militaires américains par des messages anti-américains et anti-israéliens pour délivrer des messages sur la cause palestinienne. Nous relevons conséquemment que les délinquants correspondant à ce profil de cyberdélinquance présentent des motivations intrinsèques.

5.4 Autres interprétations

Dans les précédentes études sur la cybercriminalité, il fut constaté que les victimes proviennent davantage des pays émergents que des pays développés (Norton 2011). Les résultats obtenus ne nous permettent pas de confirmer cette conclusion. Il semble que les victimes d'Amérique du Nord visent majoritairement ce même territoire. Ceci se veut peu discriminant et ne nous donne pas une image plus claire de l'origine du délinquant en tant que facteur explicatif de la provenance des victimes ciblées. Toutefois, selon la distribution observée dans le Tableau III , nous pouvons émettre l'hypothèse que l'attrait des délinquants

pour les victimes provenant d'Amérique du Nord peut s'expliquer par la disponibilité des ressources ainsi que la présence de données importantes, notamment les données gouvernementales des États-Unis qui sont fréquemment visées par les cyberdélinquants. De plus, il est plus gagnant pour des délinquants de viser des territoires où il y aura davantage de ressources financières à frauder que des territoires où l'économie est précaire et où il sera plus difficile d'en retirer un certain bénéfice.

En ce qui concerne les délinquants en provenance d'Amérique du Nord, leur profil semble plutôt discret et subtil. Les résultats significatifs se font rares. Les délinquants d'Afrique/péninsule Arabique sont plus susceptibles d'avoir un très faible degré de compétence que ceux en provenance d'Amérique du Nord, ce qui peut être mis en parallèle avec l'accessibilité aux outils technologiques et la facilité d'accès à Internet, qui permettra au délinquant en provenance d'Amérique du Nord de commettre des délits plus développés et demandant plus de compétences technologiques que les délinquants d'Afrique qui auront un accès restreint aux outillages technologiques. Comment se fait-il qu'aucun résultat significatif ne soit réellement en lien avec nos différentes hypothèses pour les délinquants d'Amérique du Nord? Afin de mieux comprendre, voici deux cas différents identifiés quant aux délinquants en provenance de l'Amérique du Nord. Un des pirates informatiques au profil plutôt atypique est originaire de ce territoire. Ce dernier est surnommé JH et est âgé de 12 ans. Il a modifié la page d'accueil d'un site Internet lors du printemps étudiant de 2012. Sa motivation n'était pas idéologique. Le groupe Anonymous lui proposait des jeux vidéo s'il leur offrait ses services. Prenons aussi pour exemple le cyberdélinquant Christopher Chaney, 35 ans, qui infiltrait les ordinateurs de célébrités afin d'obtenir des photos d'elles dévêtues. La situation des habitants

d'Amérique du Nord semble plus stable au niveau économique, politique et social que les autres territoires ou tout simplement, la criminalité semble être plus diversifiée pour ce territoire. Ceci aura pour effet de ne pas ressortir de la masse dans le cadre de tests statistiques de comparaisons.

CONCLUSION

Notre mémoire avait pour objectif de répondre à quelques questions, qui rappelons-le, étaient les suivantes : Est-ce que des différences subsistent quant aux profils des cyberdélinquants à l'échelle internationale? En quoi l'origine d'un délinquant peut-elle influer sur les caractéristiques du crime, les caractéristiques personnelles des cyberdélinquants ainsi que les caractéristiques motivationnelles? La rapidité d'Internet ainsi que l'accès aux outils technologiques seront-ils des éléments en lien avec ce phénomène ainsi que les choix des cybercriminels? Qu'en est-il des inégalités économiques, notamment au niveau des revenus?

Afin de répondre à cet objectif, nous avons réalisé différentes étapes en débutant par la recension de la littérature. Cette revue a d'abord permis d'établir les définitions de la cybercriminalité ainsi que des divers types de crimes. Ensuite, elle aura permis d'identifier divers profils de cyberdélinquants ainsi que les caractéristiques qui leur sont généralement attribuées, notamment au niveau du degré de compétence, du type de délit et du type de motivation, taxonomies qui ont d'ailleurs servi pour les analyses de la présente recherche. Nous avons également pu prendre en compte l'ampleur de ce type de criminalité, ce qui justifie l'importance que nous devons accorder dans l'approfondissement des recherches quant à cette problématique. Dans une optique préventive, il est primordial d'avoir une bonne connaissance des diverses caractéristiques de cette criminalité. Effectivement, cela permettrait d'appliquer les outils et les moyens nécessaires pour réduire les dommages ou tout simplement, empêcher cette forme de criminalité à prendre de l'ampleur. D'ailleurs, comme Internet est accessible au niveau mondial et que les délits sont majoritairement commis outre-mer, il est difficile pour un corps policier de réagir, d'autant plus que le criminel est rarement connu et que les victimes ne déclareront majoritairement pas l'évènement. Or, aucune étude n'a essayé de voir s'il existait une relation entre les différentes variables (délit, motivation, compétence, etc.) ni si les profils dégagés de

ces relations diffèrent en fonction de l'origine des cybercriminels. Comme il existe peu de connaissances quant aux caractéristiques des cyberdélinquants en fonction de leur origine, il était pertinent et nécessaire de créer une certaine base de notions théoriques à cet effet.

L'étape suivante était la création d'une base de données qui permettrait de répondre à nos objectifs. Or, nous avons sélectionné sur des moteurs de recherche 90 cas de cyberdélinquants dont l'arrestation fut médiatisée ou lesquels étaient recherchés, divisés selon six territoires géographiques : Amérique du Nord (N=15), Amérique latine (N=15), Australasie (N=15), Europe de l'Ouest (N=15), Eurasie (N=15) et Afrique/péninsule Arabique (N=15). Une fois la base de données complétée, nous avons réalisé des tests statistiques univariés dans le but de décrire notre échantillon. Ensuite, nous avons fait des analyses bivariées, plus précisément des tests de Kruskall-Wallis et des tests de tableaux de contingence, et ce, afin d'établir en premier lieu les relations qui existaient entre les variables à l'étude ainsi qu'en second lieu les relations existantes entre chacune des variables utilisées et la variable discriminante, soit l'origine du cyberdélinquant.

D'abord, les tests statistiques effectués entre nos variables permettent d'établir qu'il existe des relations entre certaines variables à l'étude, positives et négatives. Effectivement, suite aux croisements de ces variables nous avons obtenu des relations qui nous permettent de dégager certains profils de cyberdélinquants. Les résultats obtenus quant aux seconds tests statistiques permettent d'identifier que pour certains paramètres du crime, notamment le type de délit, le type de motivation, le type de victime, le degré de compétence et le revenu obtenu, des différences sont observées au plan international. Pour d'autres paramètres, comme la présence d'un trouble de santé mentale, l'appartenance à un groupe de cybercriminels et la

codélinquance, il n'était pas possible de se prononcer sur une différence notable, où aucune différence significative ne fut observée à l'échelle mondiale.

Ensuite, un profil est dégagé en ce qui a trait aux cyberdélinquants commettant des infiltrations informatiques. Ces derniers seraient davantage motivés par le caractère idéologique de leurs actions et cibleraient des instances gouvernementales afin de faire valoir leurs opinions. D'ailleurs, les délinquants présentant ce type de motivation sont plus nombreux à appartenir à un groupe, tels Anonymous et LulzSec. Ce profil peut s'expliquer par des caractéristiques qui diffèrent d'un territoire à l'autre, notamment la vitesse informatique ainsi que l'accès simplifié aux outils technologiques. Les pirates informatiques ayant de meilleurs accès informatiques, comme les cyberdélinquants en provenance de l'Europe de l'Ouest auront la chance de commettre des délits plus développés, tels que les infiltrations informatiques. Ils présenteront d'ailleurs un motif idéologique et intrinsèque, ceci s'expliquant par la présence de conflits et de mouvements sociaux. Ils sont effectivement significativement davantage motivés par la liberté d'expression, le droit de parole ainsi que le désir d'être entendus, tels les délinquants en provenance d'Europe de l'Ouest.

Inversement, les délinquants en provenance de pays où l'accès aux outils technologiques est réduit de par le peu de ressources, tant économiques que matérielles, n'auront pas l'opportunité de développer leurs habiletés techniques et auront par conséquent une criminalité moins élaborée. Le mode opératoire plus simpliste de ces cyberdélinquants pourrait également s'expliquer par le peu de temps qu'ils ont pour s'attaquer aux instances gouvernementales quand la survie de la famille est en jeu. Également, les cyberdélinquants en provenance des

territoires où les inégalités entre les revenus des habitants subsistent seront plus susceptibles de se tourner vers une criminalité motivée par le profit, telle la fraude, ainsi que des délits rapportant un revenu (Soullez, 2014), par exemple les délinquants en provenance d'Afrique/péninsule Arabique. Ces caractéristiques expliquent le second profil dégagé en lien avec le fil conducteur entre les délits de fraudes, la motivation en lien avec le profit et les victimes individuelles. Ce sont également les cybercriminels correspondant à ce profil qui obtiendront des revenus de leur criminalité, motivation qui se veut extrinsèque.

Il est tout de même important de soulever à nouveau que certaines variables ne sont pas en lien avec l'origine et sont mondialement homogènes, soient : la codélinquance, l'appartenance à un groupe ainsi que la présence de troubles de santé mentale. De plus, nous trouvons surprenant de n'avoir obtenu aucun résultat significatif en ce qui a trait au territoire de l'Amérique latine, outre le très faible degré de compétence et la sentence inconnue. Effectivement, tout portait à croire que les délinquants en provenance de ce territoire correspondraient au profil en lien avec les délits de fraudes, de l'attrait pour l'argent et le revenu obtenu de la criminalité. Effectivement, des inégalités entre les revenus des habitants de la région de l'Amérique latine persistent, tout comme ils ont un accès à Internet réduit. Quant aux régions de l'Amérique du Nord et de l'Australasie, nous sommes étonnés qu'aucun profil particulier ne se soit dessiné, probablement en lien avec la facilité d'accès à Internet, sa rapidité, la diversité de la criminalité observée dans ces territoires ainsi que d'une présence plus discrète de conflits politiques et sociaux.

Bien que notre étude ait permis d'établir certains profils en fonction de la provenance du cyberdélinquant, nous devons assumer qu'elle présente quelques limites et spécificités. D'abord, l'échantillon (N=90) est basé sur des cas d'arrestations de cyberdélinquants ayant été présentés dans divers médias. Il n'a pas été créé à l'aide de données policières crédibles ni de questionnaires autorapportés par les cyberdélinquants, ce qui peut entrainer certaines particularités. Effectivement, les médias publient plus couramment les histoires les plus captivantes susceptibles d'attirer davantage de lecteurs. Les cas recensés sont conséquemment des cas sérieux, présentant des délits de gravité plus importante ou de plus grande notoriété. Or, les profils découlant de nos tests statistiques représentent des cas plus typiques de ce genre de criminalité. Mentionnons également que lorsque les cas recensés ne correspondaient pas aux variables à l'étude ciblées, ils étaient rejetés, ce qui consiste en un biais de sélection. D'ailleurs, bien que notre échantillon soit plus représentatif que plusieurs études portant sur la cybercriminalité, il n'en demeure pas moins qu'il aurait été intéressant qu'il soit plus large pour que les assises de notre étude soient encore plus solides.

Ensuite, la division des territoires fut effectuée en prenant en compte des spécificités économiques, sociales et politiques. Toutefois, il aurait été intéressant de créer la base de données en fonction des pays d'origine des délinquants et non de créer un regroupement de ces derniers. Il serait effectivement pertinent que de futures recherches établissent des liens entre les variables, mais ce, en fonction du pays d'origine du délinquant plutôt que selon des territoires prédéfinis. Nous pouvons toutefois lire les résultats obtenus des tests statistiques en appliquant un recul et en considérant les différences établies au plan mondial afin d'enrichir nos connaissances, bien qu'ils soient teintés d'une surreprésentation médiatique.

Également, nous pouvons penser que davantage de résultats auraient été statistiquement significatifs si nous n'avions pas procédé à l'ajustement Bonferroni. Il est donc possible que nous ayons restreint la diversité des profils identifiés en tentant de diminuer les chances que des erreurs de type 1 résultent de nos tests. Il n'en demeure pas moins qu'il est intéressant de voir qu'il existe effectivement des diversités mondiales et certaines spécificités en fonction des territoires quant aux caractéristiques des cybercriminels. Par ailleurs, grâce à cette méthode, nous sommes certains de l'exactitude de ces relations.

Quant aux études à venir, il serait pertinent d'avoir un accès à des données policières et à des sources officielles afin d'accéder à une plus grande diversité de cas de cyberdélinquance, non généralisée seulement aux cas médiatisés présentant les histoires les plus alléchantes.

Il aurait également été intéressant de s'attarder à d'autres caractéristiques susceptibles d'influencer les profils à l'échelle mondiale, soit celles liées aux systèmes de règlementations et à l'établissement des diverses lois, ce qui sera pertinent pour de futures recherches. Notamment, l'impact qu'aurait la théorie du contrôle social, soit « l'ensemble des pratiques sociales, formelles ou informelles, qui tendent à produire et à maintenir la conformité des individus aux normes de leur groupe social» (Cusson, 1983). Le moyen utilisé afin d'y parvenir est différent d'une unité géographique à l'autre, permettant de croire que selon le degré de laxisme ou de cohésion, le cybercriminel aura certaines balises et limites qu'il ne pourra franchir par peur d'être puni gravement, comparées à d'autres pays où ça ne le serait point. D'ailleurs, Cusson (1983) définit aussi la théorie du contrôle social comme étant «l'ensemble des moyens spécifiquement utilisés par les hommes pour empêcher ou

limiter le crime». Ainsi, qu'il s'agisse d'un contrôle interne ou externe, l'homme contrebalance ses impulsions d'envie de créer un délit par rapport à ce contrôle social qui peut différer d'une société à l'autre. Ces différentes théories auraient été intéressantes dans le cadre de cette étude puisque d'une société à l'autre, la culture peut créer des différences au niveau de l'apprentissage social, tout comme l'aspect punitif et coercitif sera différent. Or, puisque ces théories sont applicables différemment à chacune des régions, est-ce que cela crée des différences au niveau de la criminalité informatique dans chacune de celles-ci? En fait, il est ici possible d'émettre l'hypothèse qu'effectivement, les diversités sociales et culturelles ont un impact sur le type de criminalité puisque les individus de chacun de ces territoires géographiques auront un bagage différent, donc des objectifs et des besoins divergents. De plus, l'aspect punitif différent d'un pays à l'autre peut avoir mené à la difficulté de retrouver des cas partout dans le monde, soit à cause de moins d'arrestations ou moins de criminalité. Il sera donc intéressant de s'y attarder dans des recherches futures.

Également, le contrôle social, différent d'une région à l'autre, aurait pu avoir un effet sur la cybercriminalité ainsi que sur l'identification de divers profils. Il serait intéressant pour de futurs chercheurs de se pencher davantage sur cette caractéristique. Pour l'étude actuelle, nous n'avions pas les échelles nécessaires à une telle réalisation, tout comme la division de notre base de données nous a limités à cet effet. Peut-être qu'une recherche plus approfondie, soit à l'échelle des pays, aurait permis d'obtenir des résultats significatifs quant au rôle des lois, de la règlementation et de la culture sur le développement des jeunes délinquants informatiques ainsi que sur le type de motivation et le type de délit priorisés par ceux-ci. Ces pistes sont intéressantes et seront matière à exploration.

En définitive, nous sommes d'avis que l'objectif de recherche fut atteint. Les réponses à nos questionnements ne sont que partielles de par l'importance de ce sujet, mais il nous est tout de même possible d'appliquer nos résultats avec attention à l'échelle mondiale, une force de cet ouvrage. Malgré les limites déjà relevées, soit les critères de division des territoires géographiques, le risque de généralisation en raison d'un échantillonnage peu élevé, le biais de sélection lors de la création de la base de données ainsi que le manque de connaissances quant à ce sujet, cette recherche exploratoire a permis d'établir de bonnes assises quant à l'origine en tant que facteur explicatif de la cybercriminalité de par une base de données mondiale. Le présent mémoire aura généré de nouveaux avancements au niveau des connaissances sur la cybercriminalité en établissant différents profils de cyberdélinquants et ce, en fonction de leur territoire d'origine. Il pourra apporter une optique de prévention différente pour les corps policiers ou les entreprises de protection, en générant des outils adaptés aux différents profils identifiés.

RÉFÉRENCES

Adamski, A. (1999). Crimes related to the computer network. Threats and opportunities: A criminological perspective. *Retrieved October*, *15*, 2001.

Akamai (2013). The state of the Internet. *3rd quarte,* 6:3, 1-40.

Agnew, R., Keith, S.M., Bucher, J., Welcher, A.N. et Keyes, C. (2008). Socioeconomic status, economic problems and delinquency. *Youth and society*, 40:159-181.

American Bar Association (1984). Report on Computer Crime: June 1984. Chicago: Task Force on Computer Crime, Section sur la justice criminelle.

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M. J. et Levi, M. (2012) Measuring the cost of cybercrime. *The economics of information security and privacy*, 265-300.

Arte (2011). Le dessous des cartes. Repéré à : http://ddc.arte.tv/nos-cartes/cartographie-mondiale-des-religions

Auray, N. et Kaminsky, D. (2006). Les trajectoires de professionnalisation des pirates : la double vie des professionnels de la sécurité. *Working papers in economics and social sciences*, *Annales Des Télécommunications*, 62 (11-12), 1312-1326.

Baratta, A. (1982). Conflit social et criminalité. Pour la critique de la théorie du conflit en criminologie. *Déviance et société*, 6 (1), 1-22.

Benillouche, J. (2010, 21 novembre). Comment le virus Stuxnet s'en est pris au programme nucléaire Iranien. SlateFr. Repéré à : http://www.slate.fr/story/30471/stuxnet-virus-programme-nucleaire-iranien

Best, J., & Luckenbill, D. (1981). Organizing deviance. *Prentice Hall.*

Birk, D., Gajek, S., Grobert, F., et Sadeghi. A. (2007). Phishing phishers- observing and tracing organized cybercrime. *Computer Society*, 1-6.

Britz, M.T. (2008). A new paradigm of organized crime in the United States: Criminal Syndicates, Cyber-gangs, and the worldwide web. *Sociology compass*, 2 (6), 1750-1765.

Chandler, A. (1996). The changing definition and image of hackers in popular discourse. *International Journal of the Sociology of Law*, *24*(2), 229-251

Chantler, N. (1996). Profiles of a Computer hacker. Florida: Inforwar.

Cheng, R. et Reisinger, D. (2012, 6 mars). Lulzsec arrests deal blow to hacker group. *C/Net*. Repéré à: https://nakedsecurity.sophos.com/2011/07/20/arrests-lulzsec-anonymous-hacker-suspects/

Chiesa, R., Ciappi, S., et Ducci, S. (2007). Profiling hackers. *CRC Press, Taylor et Francis Groupe Publications*.

Cluley, G. (2011, 29 juillet). Lulzsec and Anonymous hacker suspects arrested by US, UK and Dutch Autorities. *Naked Security*. Repéré à: https://nakedsecurity.sophos. com/2011/07/20/arrests-lulzsec-anonymous-hacker-suspects/

Cohen, L.E. et Felson, M. (1979). Social change and crime rate trends: a routine activity approach. *American sociological review*, 44, 588-608.

Coleman, G.E. et Golub, A. (2008). Hacker practice Moral genres and the cultural articulation of liberalism. *Anthropological Theory*, *8*(3), 255-277.

Colin, A. (2012). Les entreprises complices et victimes de la «cyberguerre*». Revue internationale et stratégique.* 3 (87), 65-72.

Copes, H. et Vieraitis, L. (2007). Identity theft: assessing offenders' strategies and perception of risk. *National institute of justice*, 1-86.

Cusson, M. (1983). Le contrôle social du crime. *Collection Sociologies*, 342 p.

Cybercriminalité : survol des incidents et des enjeux au Canada. Repéré à : http://www. rcmp-grc.gc.ca/pubs/cc-report-rapport-cc-fra.htm#sec3

Deci, E.L. et Ryan, R.M. (2010). Self-Determination. *Corsini Encyclopedia of Psychology*. 1–2.

Dix ans de conflit (2006). *Un monde diplomatique*, *cahier Kosovo*. Repéré à : http://www.monde-diplomatique.fr/cahier/kosovo/chronoyougo

Dhamija, R., Tygar, J.P. et Hearst, M. (2006). Why hameçonnage works. *Proceedings of the SIGCHI conference on Human Factors in computing systems*, 581-590.

Dupont, B. (2012). Skill and trust: a tour inside the hard drivers of computer hackers. *Université de Montréal*. 1-51.

Duffin, M., Keats, G. et Gill, M. (2006). Identity theft in the UK: The offender and victim perspective. *Perpetuity Research & Consultancy international*, 42 p.

En Ukraine, la guerre cybernétique a déjà commence (2014, 16 mars*). L'OBS/actualité*. Repéré à : http://tempsreel.nouvelobs.com/topnews/20140316.AFP2441/en-ukraine-la-guerre-cybernetique-a-deja-commence.html

Eurostat (2013). Eurostat regional yearbook 2013. Repéré à :http://epp.eurostat.ec.europa.eu/ cache/ITY_ OFFPUB/KS-HA-13-001-01/EN/KS-HA-13-001-01-EN.PDF

Franklin, J., Perrig, A., Paxson, V. et Savage, S. (2007). An inquiry into the nature and causes of the wealth of internet miscreants. *ACM conference on Computer and communications security,* 375-388.

Fox, W. (1999). Sciences sociales- Méthodes statistiques. *Méthodes des sciences humaines*. 374 p.

Goodell, J. (1996). The cyber thief and the samurai. *New York: Dell Publishing*.

Google News (2014). À propos de Google Actualités. Repéré à : https://support.google.com/news/answer/106259?hl=fr-CA&ref_topic=2428790

Grand dictionnaire de l'Office québécois de la langue française. Fiche terminologique. Repéré à :http://www.granddictionnaire.com /fiche Oqlf.aspx?Id_Fiche=2074397

Pirates News (2014). About Us. Repéré à: http://thehackernews.com/p/authors.html

Herley, C. et Florêncio, D. (2008). A profitless endeavor: phishing as tragedy of the commons. *Proceedings of the 2008 workshop on New security paradigms*, 59-70.

Hollinger, R.C. (1991). Hackers: computer heroes or electronic highwaymen?.*ACM SIGCAS Computers and Society*, *21*(1), 6-17.

Holt, T.J. et Kilger, M. (2008). Techcrafters and makecrafters: a comparison of two populations of hackers. *Computer Society*, 67-78.

Holt, T.J. et Bossler, A.M. (2013). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, 35(1), 20-40.

Holt, T.J. et Schell, B.H. (2010). Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications. *Information science reference,* 365, 16-8.

Holt, T.J. (2007). The market for Malware. *Department of criminal justice*.

Holt, T.J. (2009). Lone Hacks or group cracks: Examining the social organization of computer hackers. *American society of criminology*, 17, 336-355.

Howard, J. D. (1997). An analysis of security incidents on the Internet 1989-1995. Carnegie-Mellon Univ Pittsburgh PA.

Iiegems, M. (2014, 5 mars). Cyber-attaques en Ukraine: "La Russie bloque le trafic téléphonique mobile en Crimée". *Data News*. Repéré à : http://datanews.levif.be/ict/actualite/cyber-attaques-en-ukraine-la-russie-bloque-le-trafic-telephonique-mobile-en-crimee/article-normal-293441.html

Jackson, J.E. (1994). Fraud master: professional credit card offenders and crime. *Criminal Justice Review* , 19(1), 24-55.

Jagadic, T.N., Johnson, N.A., Jabobsson, M. et Mencser, F. (2007). Social hameçonnage. *Communications of the ACM*, 50 (10), 94-100.

Jordan, J. et Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*(4), 757-780.

Jordan, T. (2008). Hacking, Digital media and society series. *Policy press*. 160 p.

Jouan-Flahault, C., Casset-Semanez, F. et Minini, P. (2004). Du bon usage des tests dans les essais clinique. *M/S : médecin sciences*, 20 (2), 231-235.

Kshetri, M. (2006). The simple economics of cybercrimes. S*ecurity & Privacy, IEEE,* 4(1), 33-39.

Koops, B-J. (2011). The Internet and its Opportunities for Cybercrime. *Tilburg Institute for Law, Technology, and Society (TILT),* 1, 735-754.

La Banque Mondiale (2014). Données des pays et territoire. Repéré à : http://donnees.banquemondiale.org/pays

Lakhani, K.R. et WOQLF, R.G. (2005). Why hackers do what they do: understanding motivation and effort in free/open source software projects. *MIT Press*, 1-27.

Landreth, B., et Rheingold, H. (1985). *Out of the inner circle: a hacker's guide to computer security*. Bellevue, Washington: Microsoft Press.

Larousse (2014). Irlande du nord, Histoire. Repéré à: http://www. larousse.fr/encyclopedie/ divers/Irlande_du_Nord_histoire/185861

Larousse (2015). Motivation. Repéré à : http://www.larousse.fr/dictionnaires/francais/ motivation/52784

Levy, S. (2001). Hackers: Heroes of the computer revolution. *New York: Penguin Books*, 4.

Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime*, 13 (2), 71-94

Leblanc, M. (2006). Histoire naturelle de l'insomnie et identification de facteurs de risque (Doctorat dissertation, Université Laval).

Leeson, P.T. et Coyne, C.J. (2005). The economics of computer hacking. *Journal of law, Economics and policy*, 1 (2), 511-532.

Leroux, M (2013). Religion et homicide : étude du taux d'homicide des pays du monde en fonction des variables mesurant la religion et la pratique religieuse. *Université de Montréal*, Repéré à : : http://hdl.handle.net/1866/10012

McCusker, R. (2007). Transnational organised cyber crime: distinguishing threat from reality. *Crime, law and social change,* 46(4-5), 257-273.

Merton, R.K. (1938). Social structure and anomie. *American Sociological Review,* 3 (5), 672-682.

Meyer, G.R. (1989). The social organization of the computer underground. *Creative commons*, 1-76.

Moon, B., McCluskey, J. et McCluskey C.P. (2010). A general theory of crime and computer crime: An empirical Test. *Journal of Criminal Justice*, 38(4), 767-772.

Morris, R.G. et Blackburn, A.G. (2012). Cracking the code: an empirical explication of social learning theory and computer crime. *Journal of crime and justice*, 31 (1), 1-34.

Morris, R.G., Johnson, M.C., et Higgings, G.E. (2009). The role of gender in predicting the willingness to engage in digital piracy among college students. *Criminal justice studies*, 22(4) 393-404.

Mucchielli, L (2002). Les homicides. *Crime et sécurité. L'état des savoirs*, 15, 148-157.

Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New media & society*, 6(2), 195-217.

OECD (2012). OECD Internet Economy Outlook 2012, *OECD publishing*. Repéré à: http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/oecd-internet-economy-outlook-2012_9789264086463-en#page3

Ohayon, M.M. (2000). Prevalence of hallucinations and their pathological associations in the general population. *Psychiatry Research*, 97(2), 153-164.

Ouimet, M. (2011). Un monde d'homicides. *Champ pénal/Penal field*, *8*.

Padhye, V. et Gujar, M. (2012). Virtual impersonation by antisocial personalities in cybercrime. *DAV International Journal of Science.* 2(1), 49-52.

Parker, D. (1998). Fighting computer crime: A new framework for protecting information. New York: John Wiley & Sons. Inc.

Peliks, G. (2013). La cybercriminalité, un libre blanc de Forum ATENA. Repéré à : http://www.forumatena.org/files/livresblancs/LaCybercriminalite.pdf

Power, R. (1998). Current and future danger. *Computer Security Institute, San Francisco, California*.

PriceWaterHouse Coopers, L. L. C. (2013). *Key findings from the 2013 US state of cyber-crime survey."*. Technical report. June 2013. https://www. pwc. com/en_US/us/increasing-iteffectiveness/publications/assets/us-state-of-cybercrime. pdf.

Rapport de la cybercriminalité (2011), *Norton*. Repéré à : http://ca-fr.norton.com/cybercrimereport

Richardson, R. (2010). Computer Crime ans Security Survey. *CSI computer security institute.*

Roger, M.K. (2006). A two-dimensional circumplez approach to the development of a hacker taxonomy. *Digital investigation*, 3(2), 97-102.

Rogers, M.K. (2010). The Psyche of Cybercriminals: A Psycho-Social Perspective. *Cybercrimes: A Multidisciplinary Analysis,* 14, 217-235.

Ross, A. (2014). Les cyberattaques de la Russie contre l'Ukraine : comment déclarer la guerre sans vraiment la déclarer. Le huffington post. Repéré à : http://www.huffingtonpost.fr/alec-ross/les-cybers-armes-de-la-russie-frappent-lukraine-comment-declarer-la-guerre-sans-vraiment-la-declarer_b_4939969.html

Smith, R., Grabosky, P., & Urbas, G. (2004). Cyber criminals on trial. *Criminal Justice Matters*, *58*(1), 22-23.

Saumet, M. (2015, 14 janvier). Mais qui sont vraiment les anonymous?. Citizen post. Repéré à : http://citizenpost.fr/2015/01/qui-sont-vraiment-les-anonymous/

Microsoft (2014). Securité et vie privée, repéré à : http://www.microsoft.com/fr-fr/security/pc-security/botnet.aspx

Schell, B. et Dodge, J. (2002). The hacking of America*. Quorum Books*. 308 p.

Schell, B. et Martin, C. (1952). Cybercrime: A reference handbook. *Contemporary world issues*

Schell, B.H. (2007). The Internet and Society: A Reference Handbook. *Contemporary world issues*

Simon, L. (2005). Éthique Hacker et Management. *HEC Montréal*. 20 p.

Skinner, W.F. et Fream, A.M. (1997). A social learning theory analysis of computer crime among college students. *Journal of research in crime and delinquency*, 34:495.

Smith, R., Grabosky, P. et Urbas, G. (2004) Cyber Criminals on Trial, *Criminal Justice Matters*, 58:1, 22-23.

Soullez C. (2014). Criminalité et économie : un mariage efficace et durable. *La découverte*. 1 (14), 89-102.

Shulman, A. (2010). The underground credentials market. *Computer Fraud & Security*. 2010(3), 5-8.

Taylor, P.A. (1999). Hackers: Crime in the digital sublime. *Psychology press*, 198p.

Telus-Rotman (2013). IL Security Study. Rotman school of management. 1-25.

Turgeman-Goldschmidt, O. (2008). Meanings that hackers assign to their being a hacker. *Internationnal journal of cyber criminology*, 2(2), 382-396.

Union Internationale des Télécommunications (2014), Repéré à : http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Untersinger, M. (2012, 30 mai). Le virus Flame, nouvelle arme d'État dans la «cyberguserre». *L'OBS avec Rue 89*. Repéré à : http://rue89.nouvelobs.com/2012/05/29/le-virus-flame-nouvelle-arme-detat-dans-la-cyberguerre-232564

Vercueil, J. (2014). Aux racines économiques du conflit ukrainien. *Le Monde diplomatique*, *61*(724), 4.

Virus Stuxnet : le nucléaire iranien visé par la cyberguerre? (2010, 27 septembre*). L'OBS avec rue 89*. Repéré à: http://rue89.nouvelobs.com/2010/09/27/virus-stuxnet-le-nucleaire-iranien-vise-par-la-cyberguerre-168488

Van Beveren, J. (2001). A conceptual model of hacker development and motivations. *Journal of E-Business*, 1(2), 1-9.

Verizon risk team (2012). 2012 data breach investigations report.

Wall, D.S. (2003). Crime and the internet. *Routledge*, 240 p.

Wall, D.S. (2009). Organized crime and the organization of cybercrime. *University of Leeds.*

Woo, H-J. (2003). The hacker mentality: exploring the relationship between psychological variables and hacking varieties. *Université de Gioergie*. 1-120.

Wori, O. (2104). Computer crimes: factors of cybercriminal activities. *International Journal of Advanced Computer Science and Information Technology*. 3 (1): 51-67.

Yar, M. (2005). Computer hacking: just another case of juvenile delinquency? *The howard journal*, 44(4), 387-399.

Young, R., Zhang, L, et Prybutok, V.R. (2007). Hacking into the minds of hackers. *Information systems management*, 24(4), 281-287.

2011 piracy study (2011). *The software alliance*. Repéré à: http://globalstudy.bsa.org/2011/#

ANNEXE 1

SITES INTERNET CONSULTÉS

ABC News
http://abcnews.go.com/Technology/story?id=119423

Al Arabiya News
http://english.alarabiya.net/articles/2012/01/06/186713.html

Algérie Focus
http://www.algerie-focus.com/blog/2013/05/hamza-bendelladj-alias-le-hacker-souriant-risque-jusqua-30-ans-de-prison/

Algérie 360
http://www.algerie360.com/algerie/hamza-bendelladj-24-ans-accuse-de-vol-de-documents-confidentiels-%C2%ABle-hacker-souriant%C2%BB-extrade-vers-les-etats-unis/

Asia One Singapore
http://news.asiaone.com/news/singapore/businessman-admits-istana-and-pmo-website-intrusions

BBC News
http://www.bbc.com/news/technology-22079709

Biography
http://www.biography.com/people/julian-assange-20688499

Bolingbrook Patch
http://patch.com/illinois/bolingbrook/2-ghana-nationals-living-in-bolingbrook-nabbed-in-credit-card-fraud-case-police

Computer Weekly
http://www.computerweekly.com/news/2240182097/US-jails-Lulzec-hacker-Cody-Kretsinger

Computer World
http://www.computerworld.com/article/2486708/cybercrime-hacking/officials--two-people-
http://www.computerworld.com/article/2533517/networking/mafiaboy-grows-up--a-hacker-seeks-redemption.html

Canoë
http://fr.canoe.ca/infos/societe/archives/2012/10/20121018-141708.html

Daily Mail

http://www.dailymail.co.uk/news/article-2056437/Hackerazzi-suspect-Christopher-Chaney-pleads-guilty-hacking-celebrity-emails-stealing-nude-photos-Scarlett-Johansson.html
http://www.dailymail.co.uk/news/article-2111020/Top-members-hacking-groups-Anonymous-LulzSec-arrested-leader-Sabu-turns-in.html

Daily news India
http://www.dnaindia.com/india/report-cbi-takes-hacker-amit-vikram-tiwari-to-delhi-probes-his-link-with-celebrity-hacker-guccifer-1957125

Dark Reading
http://www.darkreading.com/attacks-and-breaches/lulzsec-hacker-ryan-cleary-to-be-released/d/d-id/1110361?

Discovery
http://dsc.discovery.com/tv-shows/curiosity/topics/10-famous-hackers-hacks.htm

Finding Dulcinea
http://www.findingdulcinea.com/news/on-this-day/July-August-08/On-this-Day--Robert-Morris-Becomes-First-Hacker-Prosecuted-For-Spreading-Virus.html

France 24
http://www.france24.com/fr/20131107-amazon-drogue-silk-road-retour-fbi-internet-tor-dread-pirate-roberts-ulbricht

Fun Informatique
http://www.funinformatique.com/fbi-ajoute-5-hacker-sa-liste-des-cybercriminels-les-plus-recherches/

Génération nouvelles technologies
http://www.generation-nt.com/hacker-nasa-gary-mckinnon-extradition-usa-actualite-1640732.html
http://www.generation-nt.com/hacker-nasa-lauri-love-us-army-mckinnon-actualite-1807592.html

Global Times
http://www.globaltimes.cn/content/830478.shtml#.UvKeDPl5N9c

Google
http://www.google.ca/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&sqi=2&ved=0CDsQFjAD&url=http%3A%2F%2Farchives.radio-canada.ca%2Fsante%2Fcriminalite_justice%2Fclips%2F13085%2F&ei=Nik1VabaIcPisAXC64DoCg&usg=AFQjCNHZUT-LM2XmacCv-sJ8RmdVJFxKBQ&bvm=bv.91071109,d.b2w
http://www.google.com/hostednews/afp/article/ALeqM5jo0tLZBaryWy0Zf4DXz65k5FMpPw?docId=694f1594-87ff-477a-9f5c-552f843a69c6
http://www.google.ca/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDEQFjAB&url=http%3A%2F%2Fwww.justice.gov%2Fusao%2Fnys%2Fpressreleases%2FJune12%2Fcard

shop%2Fjueshengleejasoncomplaw.pdf&ei=gSw1VYeHHq6HsQTXGA&usg=AFQjCNEj_R5jxHmu3dECwDh62BRH75E6BQ

Hackers Media
http://www.hackersmedia.com/2012/06/hacker-mrbadoo-arrested-by-fbi-last.html

Hackread
https://www.hackread.com/6-anonymous-hackers-arrested-by-dominican-republic-police/

Huffington post
http://www.huffingtonpost.com/2012/03/07/donncha-o-cearbhaill-hacker-fbi-ireland_n_1326998.html
http://www.huffingtonpost.ca/2013/04/18/cody-kretsinger-lulzsec-hacker-sentence_n_3113290.html
http://www.huffingtonpost.fr/2012/05/04/chris-chaney-piratage-emails-stars-photos_n_1476867.html
http://www.huffingtonpost.com/2013/11/13/jared-james-abrahams-pleads-guilty_n_4267799.html

IMBD
http://www.imdb.com/name/nm2238804/bio

International
http://www.lesoftonline.net/articles/une-caverne-d%E2%80%99ali-baba-%C3%A0-kinshasa-d%C3%A9tournait-nos-appels-internationaux-mobiles

International Business Times
http://www.ibtimes.co.uk/lulzsec-fbi-anonymous-hacker-irish-security-312014

In2East Africa
http://in2eastafrica.net/argentina-arrests-teen-hacker-who-netted-50000-a-month/

I Web Africa
http://www.itwebafrica.com/security/511-nigeria/231682-nigerian-govt-website-hacker-arrested

IT Espresso
http://www.itespresso.fr/le-createur-du-jailbreak-rejoint-apple-pour-un-stage-45350.html

IT Worl Canada
http://www.itworldcanada.com/article/venezuelan-arrested-for-01-airforce-hacks/12458

IT Security
http://www.itsecurity.com/features/top-10-famous-hackers-042407/

Jeune Afrique
http://www.jeuneafrique.com/actu/20131007T123417Z20131007T123351Z/

Journal du Net
http://www.journaldunet.com/solutions/0701/070117-hackers-celebres/2.shtml

Krebs on security
http://krebsonsecurity.com/2011/11/malware-click-fraud-kingpins-arrested-in-estonia/
http://krebsonsecurity.com/2013/01/inside-the-gozi-bulletproof-hosting-facility
http://krebsonsecurity.com/2013/04/phoenix-exploit-kit-author-arrested-in-russia/
http://krebsonsecurity.com/2013/01/three-men-charged-in-connection-with-gozi-trojan/
http://krebsonsecurity.com/2013/08/pavel-vrublevsky-sentenced-to-2-5-years/
http://krebsonsecurity.com/tag/paunch/

La Presse
http://www.lapresse.ca/le-nouvelliste/justice-et-faits-divers/201310/17/01-4700475-de-nouvelles-accusations-contre-un-presume-pirate-informatique.php
http://www.lapresse.ca/le-nouvelliste/justice-et-faits-divers/201302/22/01-4624494-un-presume-pirate-informatique-arrete.php

Le Figaro :
http://www.lefigaro.fr/international/2013/11/08/01003-20131108ARTFIG00583-le-hacker-de-
http://www.lefigaro.fr/international/2013/11/08/01003-20131108ARTFIG00583-le-hacker-de-l-amour-recherche-par-le-fbi.php

Le Grand Soir
http://www.legrandsoir.info/au-proces-de-bradley-manning-adrian-lamo-raconte-ses-six-jours-de-discussions-avec-l-accuse-the-guardian.html
http://www.legrandsoir.info/declaration-de-jeremy-hammond-hacker-anarchiste-et-anti-guerre-condamne-a-10-ans-de-prison.html

Le Monde
http://www.lemonde.fr/disparitions/article/2013/07/29/mort-du-hacker-barnaby-jack-detrousseur-de-distributeur_3454728_3382.html
http://www.lemonde.fr/technologies/article/2012/03/07/le-pirate-sabu-tombe-le-masque_1653224_651865.html

Le Parisien
http://www.leparisien.fr/faits-divers/arrestation-du-hacker-le-plus-recherche-de-france-10-07-2003-2004239529.php

Le Républicain Lorrain
http://www.republicain-lorrain.fr/actualite/2013/11/14/le-pirate-je-suis-un-geek-mais-j-achete-mes-cd

Le Soir
http://www.lesoir.be/344788/article/belgium-iphone/2013-10-21/hacker-pod2g-prouve-qu-il-est-possible-d-intercepter-des-imessage

L'Express
http://www.lexpress.fr/actualite/societe/justice/un-jeune-hacker-condamne-a-un-million-d-euros-de-dommages-et-interets_1298832.html#xtor=AL-447

Liberty Helena
http://libertyhelena.wordpress.com/tag/duygu-kerimoglu/

Los Angeles Times
http://articles.latimes.com/1995-08-19/business/fi-36656_1_citibank-system

Metro News
http://www.metronews.fr/high-tech/le-hacker-leader-de-lulzsec-matt-flannery-aushok-risque-12-ans-de-prison/mmdz!dSPAAyI2TdKDE/

Mid Day
http://archive.mid-day.com/news/2012/mar/060312-Two-foreigners-arrested-for-hacking-bank-passwords.htm

Naked Security
https://nakedsecurity.sophos.com/2012/12/14/gary-mckinnon-escapes-charges/

Nation Multimedia
http://www.nationmultimedia.com/national/African-arrested-on-bank-hacking-charges-30213991.html

NU Data Security
http://nudatasecurity.com/blog/headlines/lulzsec-raynaldo-rivera-sentenced-for-sony-data-breach/

Numerama
http://www.numerama.com/magazine/27356-au-tribunal-un-hacker-de-12-ans-qui-se-faisait-payer-en-jeux-video.html

PC World
http://www.pcworld.com/article/2089660/officials-two-people-used-fake-credit-cards-that-may-be-linked-to-target-data-breach.html
http://www.pcworld.com/article/144473/article.html

Rediff India Abroad
http://ia.rediff.com/news/2005/sep/01suman.htm

Reuters

http://www.reuters.com/article/2012/03/09/us-cyber-arrestsmartynidUSBRE82807M20120309

SC Magazine
http://www.scmagazine.com/teen-hacker-goes-to-the-house-of-detention/article/32415/
http://www.scmagazine.com/authorities-arrest-infamous-hacker-diabl0-in-bangkok/article/338982/

Sen 360
http://www.sen360.com/style/le-pirate-du-facebook-de-selbe-ndome-condamne-agrave-six-mois-de-prison-ferme-88642.html

Slate
http://www.slate.fr/life/72777/sven-olaf-kamphuis-ennemi-public-numero-un-cyber-securite

Softpedia
http://news.softpedia.com/news/23-Year-Old-Nigerian-Arrested-for-Hacking-Government-Websites-387503.shtml

Spam Fighter
http://www.spamfighter.com/News-13764-Colombia-Seizes-Hacking-Ring-Pilfering-$2-Million.htm

Spectrum
http://spectrum.columbiaspectator.com/spectrum/fourth-suspect-in-6-million-columbia-hackin-scheme-arrested

Stuff Technology
http://www.stuff.co.nz/technology/digital-living/30013893/aaron-swartz-a-beautiful-mind

The Voice
http://www.voice-online.co.uk/article/nigerian-man-arrested-over-alleged-bank-account-hacking

The Asian Age
http://archive.asianage.com/mumbai/phishing-cop-s-account-nigerian-under-arrest-205

The federal bureau of investifation-FBI
http://www.fbi.gov/wanted/cyber
http://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-24-arrests-in-eight-countries-as-part-of-international-cyber-crime-takedown
http://www.fbi.gov/losangeles/press-releases/2013/second-member-of-hacking-group-sentenced-to-more-than-a-year-in-prison-for-stealing-customer-information-from-sony-pictures-computers
http://www.fbi.gov/losangeles/press-releases/2011/florida-man-arrested-in-operation-hackerazzi-for-targeting-celebrities-with-computer-intrusion-wiretapping-and-identity-theft

The Hackers News
http://thehackernews.com/2013/01/russian-hacker-behind-gozi-malware.html
http://thehackernews.com/2012/09/anonymous-member-barrett-brown-arrested.html
http://thehackernews.com/2012/09/pirate-bay-founder-arrested-in-cambodia.html
http://thehackernews.com/2012/06/operation-card-shop-fbi-arrested-24.html
http://thehackernews.com/2012/06/russian-botnet-hacker-arrested-for.html
http://thehackernews.com/2013/11/singapore-police-arrested-six-men-for.html
http://thehackernews.com/2012/07/russian-hacker-arrested-for-ddos.html
http://thehackernews.com/2012/10/barrett-brown-charged-with-internet.html

The Independent
http://www.independent.co.uk/news/fine-for-boy-who-hacked-into-pentagon-1274204.html
http://www.independent.co.uk/news/people/profiles/jake-davis-the-teen-hacker-who-came-in-from-the-cold-8887544.html

The Inquirer
http://www.theinquirer.net/inquirer/news/2322002/pirate-bay-founder-gottfrid-svartholm-warg-gets-an-extended-prison-stay

The New Yorker
http://www.newyorker.com/online/blogs/elements/2013/11/jeremy-hammond-and-anonymous-hacker-with-a-cause.html

The Real Singapore
http://therealsingapore.com/content/two-brothers-unrelated-james-raj-charged-over-pmo-website-hack

The Register
http://www.theregister.co.uk/2011/09/26/hidemyass_lulzsec_controversy/

The Straits Times
http://www.straitstimes.com/breaking-news/singapore/story/istana-site-hacking-businessman-and-student-arrested-20131128

The Sun
http://www.thesun.ie/irishsol/homepage/news/5188225/Students-hand-over-10000-for-hacking-Fine-Gael-website.html

The United States Department of Justice
http://www.justice.gov/opa/pr/hacker-sentenced-seven-years-prison-role-two-hacking-schemes-involving-total-more-240000
http://www.justice.gov/opa/pr/2008/April/08-crm-294.html

The Verge
http://www.theverge.com/2013/1/24/3910652/fbi-arrests-gozi-malware-masterminds

Times of India
http://timesofindia.indiatimes.com/tech/it-services/Biggest-global-hacking-network-busted-Pune-man-held/articleshow/29323641.cms

Tuniscope
http://tuniscope.com/index.php/categorie/actualites/societe/pirate-153016#.UoGSh_ldA0B

University Time Magazine
http://www.universitytimes.ie/?p=9211

Voice of America
http://www.voanews.com/content/reu-singapore-arrest-hacker-attack-government-websites/1788341.html

Voice Of Grey Hat
http://www.voiceofgreyhat.com/2012/07/RussianHackerDmitryZubakhaArrestedForDDoSAttack.html

Voice of VOIPSA
http://voipsa.org/blog/2010/02/19/voip-fraudster-and-fugitive-edwin-pena-pleads-guilty/

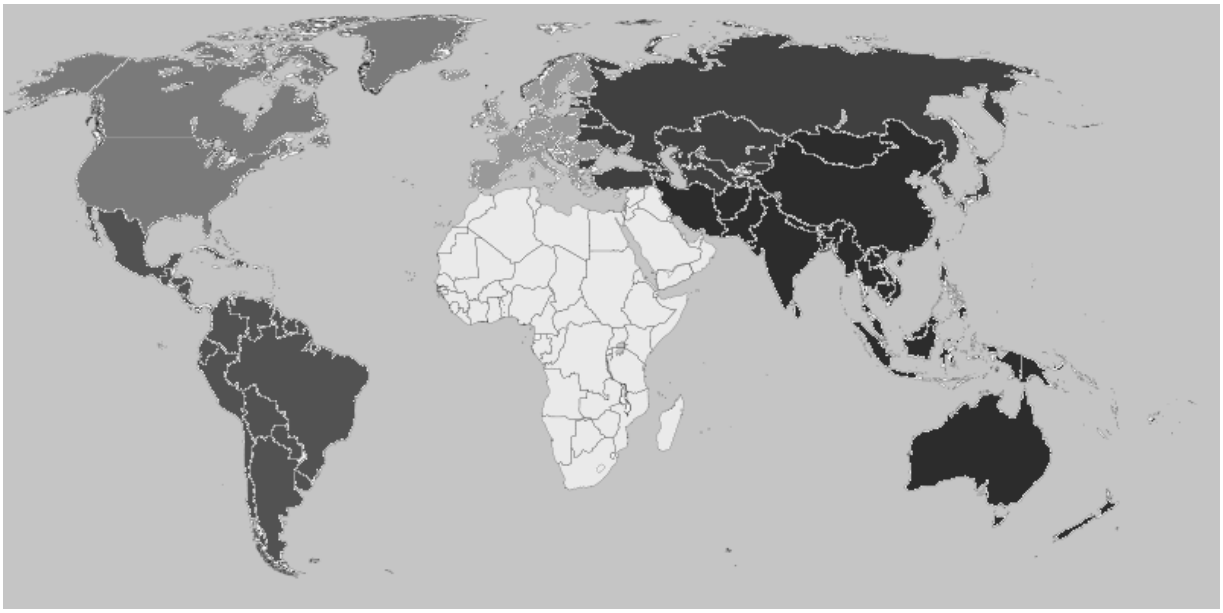
Washington post
http://www.washingtonpost.com/blogs/worldviews/post/israeli-saudi-hackers-in-confusing-credit-card-publishing-war/2012/01/12/gIQA3QCFuP_blog.html

Wikipédia
http://en.wikipedia.org/wiki/Jeanson_James_Ancheta
http://fr.wikipedia.org/wiki/LulzSechttp://www.lemonde.fr/disparitions/article/2013/07/29/mort-du-hacker-barnaby-jack-detrousseur-de-distributeur_3454728_3382.html
http://fr.wikipedia.org/wiki/Sven_Jaschan
http://en.wikipedia.org/wiki/Albert_Gonzalez
http://en.wikipedia.org/wiki/Jeremy_Hammond#Career
http://fr.wikipedia.org/wiki/Barnaby_Jack

Wired
http://www.wired.com/threatlevel/2010/07/maksik-lured-to-arrest/
http://www.wired.com/2010/05/lamo/
http://www.wired.com/threatlevel/2010/03/christopher-scott-sentencing/
http://www.wired.com/2009/06/butler_court/
http://fr.canoe.ca/infos/societe/archives/2012/10/20121018-141708.html
http://www.wired.com/2012/07/tenenbaum-sentenced/

20 minutes
http://www.20min.ch/ro/news/vaud/story/-Ririlesodomite--avait-pirat--l-ordi-de-son-ex-24210342

ANNEXE 2



Amérique du Nord :	Amérique latine :	Europe de l'Ouest :	Europe de l'Est :	Afrique/Péninsule Arabique :	Australasie
Canada États-Unis	Amérique Centrale Amérique du Sud	Allemagne Andorre Autriche Belgique Danemark Espagne Finlande France Grèce Irlande Islande Italie Liechtenstein Luxembourg Malte Norvège Pays-Bas Portugal Royaume-Uni Saint-Marin Suisse Suède ; Vatican.	Biélorussie Russie Ukraine Finlande Estonie Lettonie Lituanie Bosnie-Herzégovine Bulgarie Croatie Macédoine Monténégro Serbie Slovénie Albanie Chypre.	Pays d'Afrique Arabie Saoudite Irak Israël Iran Syrie Yémen Quatar Oman Jordanie Émirats arabes unis Liban.	Népal Afghanistan Pakistan Inde Mongolie Chine Bangladesh Thaïlande Japon Philippines Malaisie Sri Lanka Australie